

“El *firewall* sigue siendo el cerebro de la red y las medianas empresas ya no pueden preguntarse si pueden tenerlo o no”

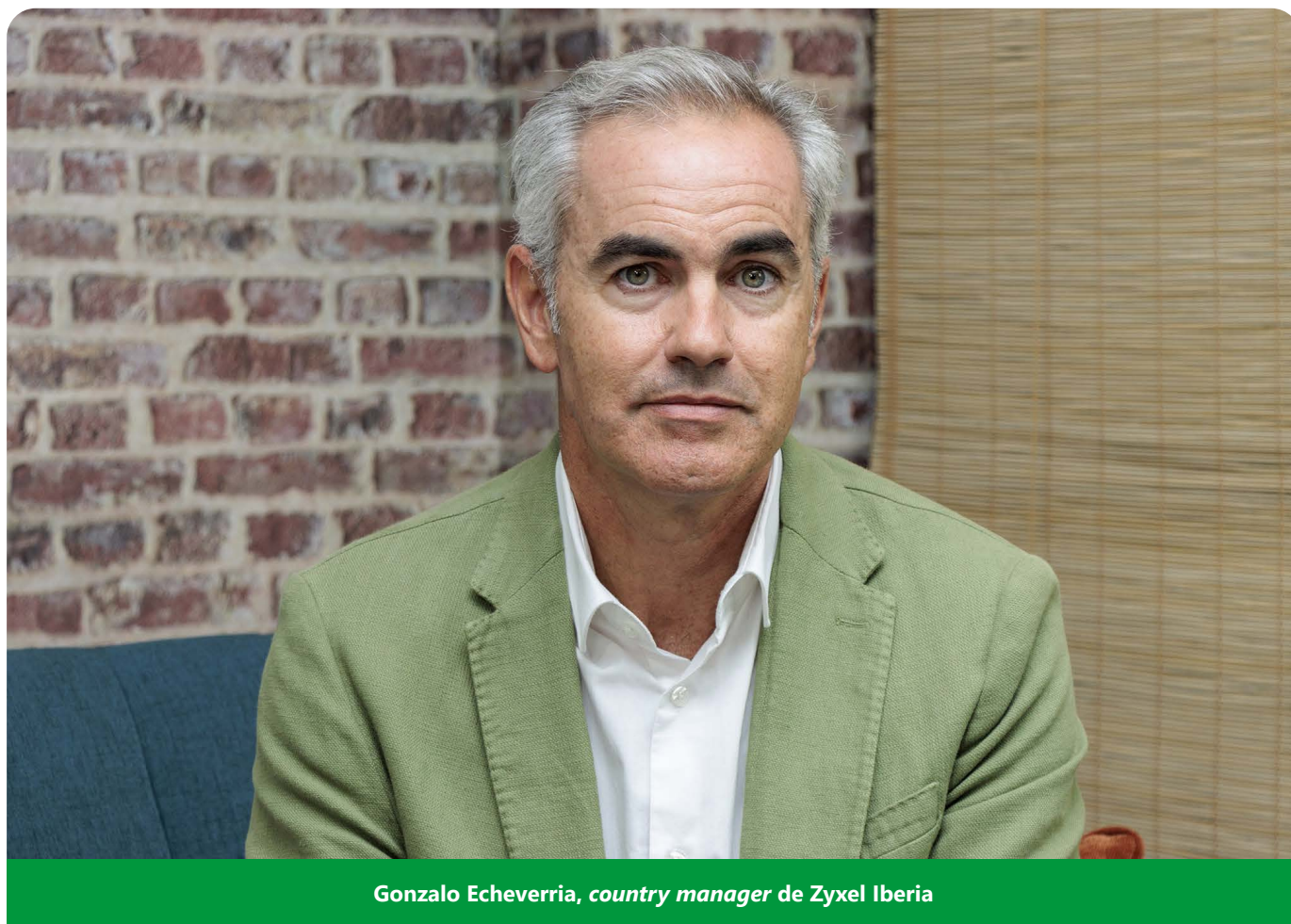


Las soluciones de red basadas en la nube aportan a las empresas una mayor seguridad y continuidad del negocio. La multinacional taiwanesa Zyxel, especializada en conmutación, conectividad inalámbrica y seguridad, contribuye a dar la máxima protección a las compañías con soluciones como la nueva serie de *firewalls* H, enfocada al segmento mediano empresarial. Gonzalo Echeverria, *country manager* de Zyxel Iberia, destaca en esta entrevista las ventajas de la compañía en el segmento de la seguridad.

Inma Elizalde

35 años de vida han permitido a la multinacional taiwanesa Zyxel conectar a más de un millón de empresas, en 150 países, impregnando con sus soluciones de red basadas en la nube a más de 100 millones de usuarios. ¿El secreto de su éxito? La facilidad de uso de unas soluciones, enfocadas a las pequeñas y medianas compañías, que aportan monitorización y visibilidad de todo lo que ocurre en la red, reconoce Gonzalo Echeverría.

En un mundo en el que los ciberdelincuentes lanzan amenazas cada vez más sofisticadas y difíciles de detectar, las medianas empresas tienen que ser conscientes del constante riesgo de ataque. Los ciberdelincuentes han evolucionado al mismo ritmo al que lo ha hecho la tecnología, haciendo de sus ataques uno de los negocios más fructíferos. En su lucha por defender al sector empresarial, la marca taiwanesa se concentró, desde el primer día, en el segmento de las pequeñas y medianas empresas, adaptando una solución, que pue-



Gonzalo Echeverría, country manager de Zyxel Iberia

de tener una gran organización, a las necesidades de las medianas. Y aportando un nivel máximo de seguridad con un precio mucho más ajustado.

Soluciones

Junto a las amenazas tradicionales suelen surgir nuevos ataques. Gonzalo Echeverría destaca que en 2024 las suplantaciones de identi-

Consejos para llevar a cabo una correcta seguridad

A la hora de llevar a cabo una correcta seguridad en el mundo de la mediana empresa Gonzalo Echeverría destaca hacer, en primer lugar, una auditoría interna con el fin de conocer, sobre todo, dónde se encuentran los datos sensibles. Una vez identificados es indispensable conocer quién accede a ellos, desde dónde y desde qué dispositivos, por lo que aconseja contar con una gestión muy clara de los permisos que se van a conceder en este sentido y realizar un reporte de cómo se van a llevar a cabo esos accesos. Todo ello sin olvidar las actualizaciones, ya que un porcentaje muy alto de ataques se producen a través de dispositivos que no han sido actualizados, algo que las empresas pueden llevar a cabo con Nebula Cloud de manera automática.

dad no han dejado de crecer. “Las empresas, al contar con usuarios en remoto y múltiples dispositivos a los que conectarse, necesitan soluciones que les permitan gestionar todos los accesos a todos los recursos de la red de la compañía, con un nivel de seguridad elevado, independientemente de que sea una pequeña o mediana organización. El nivel de seguridad

tiene que ser tan alto como el de una gran corporación”, advierte. En este sentido, señala a Nebula Cloud como la herramienta perfecta para una pyme al tener todos los elementos de red perfectamente monitorizados y actualizados. Nebula Cloud permite a las empresas conectar, proteger y gestionar sus dispositivos de una manera centralizada y eficiente. Pero no

es la única solución que ofrecen. Sus *firewalls* juegan un papel fundamental en la misma, en una evolución constante de la compañía por aportar al mercado la última innovación en ciberseguridad.

“El *firewall* sigue siendo el cerebro de la red y las pymes ya no pueden preguntarse si pueden o no tenerlo”, constata. “Hace años las empresas tenían la idea preconcebida de que un *firewall* estaba dirigido a grandes organizaciones y, que por lo tanto, no lo necesitaban cuando en realidad es todo lo contrario. Necesitan un *firewall* adaptado a su tamaño”, explica. ¿Qué ofrece Zyxel en este sentido? Un *firewall* para pequeñas o medianas empresas que se paga en función de los usuarios que van a utilizarlo o de los dispositivos que van a conectarse al mismo”, responde. Uno de sus últimos lanzamientos pasa por la nueva serie de *firewalls* H, enfocada al segmento mediano. Cuenta con anchos de banda muy superiores y velocidades en VPN muy altas, ante la

Ventajas de Nebula Cloud

- Seguridad de red con protección multicapa.
- La gestión centralizada de Nebula permite gestionar los puntos de acceso, los *firewalls* y *switches* desde una única plataforma en la nube.
- Acceso remoto desde cualquier lugar con conexión a Internet.
- Cuenta con tecnología de seguridad de los principales proveedores. Medidas de seguridad avanzadas como el cifrado de datos y autenticación multifactor. Técnicas de filtrado que evitan hasta el 70 % de las amenazas. Incluye filtrado de contenidos DNS y filtrado de reputación, eliminando los puntos oscuros.
- Altamente escalable, permitiendo a las empresas crecer y adaptar su infraestructura de red en función de sus necesidades.
- Reducción de costes al eliminar el hardware físico y su mantenimiento.
- Rápida implementación.

gran demanda de las pymes en este sentido, avanza. En definitiva, la gama H permite tener siempre gestionadas las VPN, así como todas las conexiones remotas que necesite una empresa: usuarios en oficina, remotos o en itinerancia, independientemente de los dispositi-

vos que tengan “porque las pymes cuentan con múltiples dispositivos”, apunta. En este sentido Nebula Cloud puede gestionarlos de manera sencilla, apunta.

La diferenciación de sus *firewalls* viene de la mano de la gran seguridad que aportan, de la



manera más sencilla posible. “Una pyme, independientemente de que tenga o no un departamento de IT, va a tener un acceso muy sencillo a Nebula Cloud, actualizando todos sus dispositivos de manera automática”, observa.



Aportando visibilidad

¿Cómo mejoran la visibilidad y el control sobre el tráfico de red? “La monitorización para las pymes es fundamental”, recuerda. “No hay que tener un conocimiento técnico muy alto. En un panel de control se puede ver el tráfico de los dispositivos y usuarios, permitiendo gestionar identidades y accesos a cada uno de los recursos de la empresa y de la red de manera sencilla”, argumenta.

En cuanto al retorno de la inversión, más allá

de la rentabilidad que da no tener que parar una empresa por un ataque, Gonzalo Echeverría manifiesta que recomiendan a los responsables de TI implantar un sistema que les permita estar actualizados, gestionar sus dispositivos de manera sencilla y sin costes

ocultos. “Nuestros *firewalls* tienen, al final del día, un rendimiento y una vida útil muy larga, por lo que la inversión no es elevada. Además, aportamos continuidad al negocio. Con todas estas premisas el cálculo del ROI con respecto a nuestras soluciones es sencillo”, sentencia.

Firewalls serie H de Zyxel

- Con la serie USGFLEX H, de Zyxel, las medianas empresas podrán identificar y protegerse de las ciberamenazas en tan sólo minutos.
- Con la IA y las tecnologías en la nube las empresas podrán responder ante amenazas no identificadas.
- Su seguridad web incluye funciones de filtro de contenidos que abarcan la comprobación de IP con categorías sincronizadas en la nube, actualizadas en todo momento.
- Protección contra *malware* y *ransomware*.
- Detección colaborativa que permite que los dispositivos de red trabajen juntos para bloquear o poner en cuarentena los dispositivos comprometidos en el borde de la red.
- Posibilidad de gestionar en modo local la plataforma de gestión centralizada **Nebula Cloud**.