

# Zyxel: “El firewall se ha convertido en el cerebro de la red y gestiona todo”

La evolución de Zyxel ha sido enorme en sus tres décadas de vida. Tan grande que Gonzalo Echeverría, *country manager* para España y Portugal de la compañía, reconoce que si hace unos años eran reconocidos por sus routers, hoy es su parte de seguridad la que predomina. Algo que para Echeverría es importante, si tenemos en cuenta que Zyxel se dirige a la pyme y esta siempre mantiene la eterna promesa de empezar a establecer medidas de seguridad en sus redes.

Inma Elizalde

**Zyxel ha cumplido 30 años de vida. ¿Cuáles han sido los mayores hitos conseguidos durante estas tres décadas?**

Empezamos con los modem y en los últimos diez años hemos avanzado tanto en seguridad como en *wireless* y en fibra óptica.

El lanzamiento de SD-WAN, en la parte de seguridad, supuso ofrecer servicios de *enterprise* a la pequeña y mediana empresa.

En *wireless* contamos con la gestión integrada en *cloud*, acercando también a la pyme soluciones de empresas grandes. Y en la parte de fibra óptica aca-



Gonzalo Echeverría, *country manager* para España y Portugal de Zyxel

bamos de lanzar GPON, un salto hacia adelante en redes basadas en fibra óptica.

### Zyxel está presente en 150 mercados. ¿Cuál es su punto fuerte en España?

La fuerte presencia a nivel de canal. Tenemos un equipo todavía relativamente pequeño, pero una gran presencia en el canal mayorista y en el canal integrador. Hemos crecido mucho en los últimos cinco años en integradores pequeños-medianos. Y en los últimos dos, ya estamos atacando a los grandes.

### ¿Qué es lo que más se reconoce de Zyxel en nuestro país?

La parte de seguridad. Hace diez años la respuesta habría sido la parte de *routers*. Lo bueno que tenemos es que, hablando de seguridad, hablamos del paraguas entero de toda la red. La red integrada, con *switches* y *wireless*.

### ¿Cuál es su penetración en las medianas or-

### ganizaciones y qué van a hacer para aumentar la misma?

Nuestras soluciones son tan sencillas de instalar que la pequeña empresa es la que más fácilmente se ve recompensada y le facilitamos el acceso a la seguridad.

Tenemos un *target* de hasta 1.000 empleados hacia abajo. Hablamos de pequeña y mediana, pero en realidad tenemos soluciones de *switches* y de *firewall* grandes. Estamos en grandes corporaciones, pero tenemos claro que ese no es nuestro nicho. Hay otras marcas que están en el mismo

nicho o mucho mejor posicionados, por lo que decimos que de ahí para abajo lo tenemos todo resuelto.

### ¿Cuáles son las mayores necesidades de la mediana empresa en redes?

La seguridad. Cuando nos llegan proyectos, afortunadamente ya vienen con esta demanda. Hasta hace unos años no ocurría esto. Querían renovar su red, pero la seguridad se quedaba en segundo plano, e incluso en algunos proyectos consideraban que no les hacía falta.



Hoy en día, afortunadamente, el *firewall* se ha convertido en el cerebro de la red y es quien gestiona todo.

En la pequeña y mediana empresa es fundamental poder integrar un *firewall* que gestione todos estos elementos de red.

### **Imbuidos como estamos en la transformación digital, ¿cuál es el papel que está jugando Zyxel en la misma?**

Como vendemos todavía hardware, somos la unión entre el usuario, el dispositivo y el *cloud*. Nuestra tecnología permite acceder al escritorio virtual, al *cloud*, a todos los servicios y aplicaciones, de la mejor forma posible.

### **¿Qué representa Nébula en esta transformación?**

Es una herramienta basada en *cloud* que permite tener monitorización y gestión de todos

los elementos de red. Es fundamental para todo nuestro canal, no solo para el integrador. También el usuario final puede utilizarlo porque permite utilizar múltiples niveles de administración.

### **¿Cómo ayuda a las empresas a subir a la nube?**

No tienes que tener en tu red ningún tipo de software ni de hardware específico. Vía *cloud* tienes acceso a todos los elementos. Con esta herramienta no solo gestionas, también monitorizas. La empresa no solo quiere protegerse, también saber qué es lo que está pasando.

### **¿Hasta qué punto las redes están siendo objetivo de los ciberdelincuentes?**

Si hablamos de datos nos asustamos porque se multiplican semanalmente el número de ataques y las mutaciones que están teniendo los mismos.

Las empresas ya son conscientes de que tienen que protegerse y tres de cada cuatro, en la pequeña y mediana empresa, han tenido ataques de una u otra manera. La seguridad para ellos, afortunadamente, ya es un básico. Con nosotros tienen la posibilidad de poder protegerse.

Nuestro canal está ofreciendo el servicio de seguridad. Y este servicio ya no es solo una capa

de UTM capaz de ver dónde estamos protegiendo la red del cliente a nivel perimetral. También estamos protegiendo las comunicaciones que tiene con cada uno de los elementos que hay fuera de esa red, como otras sedes de la misma empresa, usuarios remotos o el propio



cloud de todos los servicios y aplicaciones que tenga alojados en cloud.

Con nuestros firewalls van a poder gestionar esas comunicaciones para que la comunicación sea cien por cien segura.

**A medida que el IoT se vaya desplegando, los ciberdelincuentes pondrán más sus miras en el mismo. ¿Desde Zyxel van a lanzar soluciones en este sentido?**

Nuestras soluciones de seguridad son multicapa y van también para el IoT. El problema viene porque estamos multiplicando el número de posibles agujeros de la red, por lo que la protección no puede ser la misma.

Nuestras soluciones son multicapa. A medida que vayas añadiendo elementos, tienes que tener claro que tienes que separar esos tráfico y de hasta dónde puede entrar y hasta dónde no.

Es poner más complicaciones a los ciberdelincuentes.



**Usted ha comentado que a las empresas españolas les falta camino por recorrer para llegar a alcanzar las soluciones que protejan correctamente a las organizaciones. ¿Dónde está el fallo y de quién es la culpa?**

Creo que por ser una pequeña empresa no interesa a los ciberdelincuentes, pero es un gran error porque el ciberdelincuente sabe que tienes información crítica y, que si te la codifica, tienes un problema muy grave. Las empresas tienen que ser conscientes de que los ciberdelincuentes quieren su dinero y les da igual a lo que se dediquen.

Poco a poco van siendo conscientes de que realmente necesitan ir poniendo cada vez más medidas de seguridad.

**Además, incrementan su seguridad con la ayuda de otros partners. ¿Cómo pueden sus soluciones de seguridad predecir los movimientos que**

**van a hacer los ciberdelincuentes?**

Nuestra solución está integrada por soluciones de terceros porque pensamos que, en cuanto al *antispham*, filtrado de contenidos, antivirus... hay especialistas que lo van a hacer mejor que nosotros. Combinamos esos servicios con nuestro hardware. De esta manera nuestros servicios siempre estarán actualizados al 100 %.

Tenemos acuerdos de antivirus con Kaspersky. Zyxel nunca va a poder desarrollar un antivirus tan potente como Kaspersky, por lo que preferimos tener este acuerdo con ellos. Esta, junto a



Bitdefender, son las principales empresas con las que trabajamos. Se puede elegir cualquiera de las dos opciones, o las dos soluciones combinada con nuestro hardware.

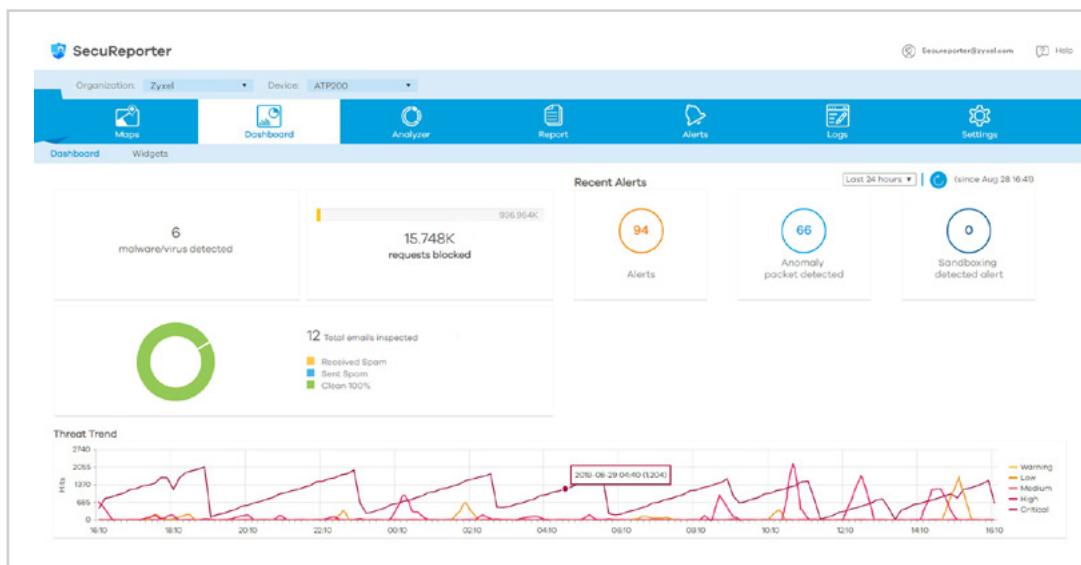
**Actualmente la red es una herramienta de inteligencia de negocio. ¿Cuál es la aportación de Zyxel en el apartado de la inteligencia artificial?**

Los últimos *firewall* que hemos lanzado, la gama ATP, ya incluyen inteligencia artificial, capa de Sandboxing, donde el tráfico es filtrado antes incluso de llegar a la red del cliente. Está aprendiendo, en función del comportamiento del *malware*, viendo el posible comportamiento de esos archivos a la hora de ejecutarlos.

**¿Cuál es su relación con el CISO?**

Afortunadamente, en la mediana empresa todo

esto lo tienen muy avanzado, pero siempre quieren tener visibilidad de lo que está ocurriendo. Quieren tener clara la monitorización. Con nuestros *firewall* tienen herramientas de monitorización en tiempo real, su reporte, su acceso por dispositivo.



Saben qué es lo que está pasando, el número de ataques que están recibiendo, de dónde vienen los mismos. Cada vez más, dan un reporte mucho más detallado para poder tomar medidas.

**¿Cuáles son las soluciones de Zyxel que no**

**deberían faltar en una mediana empresa?**

El *firewall* es el cerebro de una empresa, por lo que con el mismo van a poder establecer sus políticas de enrutamiento y priorizar o bloquear aplicaciones y definir el ancho de banda.

VPNs, cada vez más. Afortunadamente ya tenemos claro que, si quiero conectar a los servidores de la oficina desde casa, tengo que hacerlo a través de VPN. Tengo que encriptar ese tráfico. Es una seguridad básica. Y la parte de *wireless* profesional. Hoy en día se integran como parte adicional del elemento de red.

**¿Cuál es su mayor reto en el mercado español?**

Nos hemos marcado como objetivo, en la parte de seguridad de la pequeña y mediana empresa, alcanzar un 20 % de cuota de mercado para el año que viene. Actualmente estamos en torno al 13 %.

# Soluciones de Zyxel para la pyme en 2020

¿Qué ofrecerá Zyxel en 2020? Gonzalo Echeverría, *country manager* para España y Portugal de la compañía, destaca en este vídeo sus soluciones SD-ONE para la red de la pequeña y mediana empresa. ¿Cuáles son las ventajas de las mismas? Echeverría las desvela a continuación.



Gonzalo Echeverría, *country manager* para España y Portugal de la compañía