

F5 quiere fortalecer su relación con el CIO y el CISO

Haciendo un repaso en el tiempo, F5 Networks decidió añadir a su negocio tradicional conformado por el balanceo de carga y la entrega de aplicaciones, dos líneas nuevas: la seguridad y la nube. Juan Rodríguez, director general para España y Portugal de F5 Networks destaca que, aunque en el mercado son reconocidos gracias al balanceo de carga, este se convirtió con el tiempo en el denominado application delivery controller, (ADC), dotando de inteligencia a las capas superiores, hasta que el mercado comenzó a demandarles inteligencia de seguridad.

Inma Elizalde

Animan a las organizaciones a adoptar el concepto "application capital" como la mejor vía para lograr nuevos modelos de innovación y mejores resultados de negocio. ¿En qué consiste?

En el siglo XIX el factor de desarrollo de negocio en el que la gente ponía foco era en la parte física. En el siglo XX fue más la parte de desarrollo de



Juan Rodríguez, director general para España y Portugal de F5 Networks



nuevos servicios, el *outsourcing*, Ver cómo el hombre era capaz de mejorar los procesos físicos que se habían creado anteriormente. Ahora eso ya no es importante. Airbnb, la mayor cadena hotelera, no tiene ni una habitación, solo aplicaciones en todo el mundo, altamente escalables, con mecanismos de seguridad que le permiten cotizar en bolsa con el mayor valor bursátil.

Para nosotros "*application capital*" es la posibilidad de que una empresa se focalice en sus aplicaciones y sus datos y que el resto lo obtenga como una *utility*.

Otro de sus mensajes pasa porque la verdadera transformación digital solo puede ocurrir si las empresas ponen más énfasis en la modernización de los *portfolios* de las aplicaciones y de sus infraestructuras asociadas. ¿Cómo se traduce este énfasis en el mercado empresarial español?

Vemos que hay que cambiar el concepto de cómo debo desarrollar la aplicación y cómo la consumo. Las diferentes organizaciones que hay en la empresa, las personas que desarrollan código abierto y los que desarrollan las aplicaciones críticas son entornos separados. De ahí la importancia de que el CISO se alinee con la parte de estrategia. Y entender los sistemas que manejan. Entender que existen mecanismos y empresas que son capaces de llevar las cargas de aplicaciones a la nube, de una manera transparente y flexible. Ahí F5 puede ayudar a los clientes en su transformación.

"Application capital es la posibilidad de que una empresa se focalice en sus aplicaciones y sus datos y que el resto lo obtenga como una utility"

Para F5 la protección de aplicaciones es uno de los principales retos de seguridad. ¿Cuáles son las mayores vulnerabilidades a las que se enfrentan las aplicaciones en este momento?

Principalmente ataques a nivel de aplicaciones, robo de identidades, fraude... Una entidad tiene protegido su *portfolio* de aplicaciones en la nube, pero cuando alguien se conecta vía móvil y mete sus datos, nadie protege su identidad.

También vemos muchos ataques en la parte DDoS y en la de *firewall* o DNS. Con los nuevos servicios F5 *cloud* que hemos sacado en Amazon, permitimos al cliente que el DNS se lo lleve a la nube, de tal manera que la empresa mantiene su DNS en su CPD. Si le atacan, puede tener un DNS secundario en la nube, por lo que en tiempo real queda resuelto.

En breve queremos seguir desarrollando todos los servicios de aplicaciones. Contamos con servicios como Silverline, F5 Professional Services... Vamos dando al cliente la posibilidad de uso de nuestra infraestructura en



cualquier tipo de modelo de consumo que quiera.

F5 está centrada en hacer que las aplicaciones de los clientes vayan más rápido. ¿Cómo lo consiguen?

Nos situamos entre el usuario, la información y las aplicaciones del cliente. Liberamos de toda la carga a las aplicaciones del cliente. Entendemos cómo pasar la información a

las aplicaciones y tenemos mecanismos de optimización del dato, por lo que permitimos que el cliente en un momento dado, pueda priorizar tráfico y que sea nuestra infraestructura la que se encargue de optimizar y responder a esas demandas.

En la era del *multicloud* F5 se está adaptando al nuevo entorno e innovando rápidamente para ayudar a las organizaciones a hacer frente a los problemas más apremiantes relacionados con los entornos *multicloud*. ¿Cuáles son los mismos?

Es un tema de seguridad y de procesos. Hasta hace poco los clientes iban a la nube y se llevaban algunas cargas de trabajo a una nube en concreto y se producía un mecanismo tipo *locked-in* por el que los clientes no podían abandonar a ese proveedor de *cloud* durante un tiempo. Para evitarlo los clientes comenzaron a llevarse cargas de trabajo a diferentes nubes.

Un 65 % de los clientes tiene más de tres nubes privadas o públicas. Cada una de ellas tiene diferentes

entornos y mecanismos de seguridad, de gestión o acceso. Nosotros ayudamos al cliente a unificar todo esto y somos nosotros los que dialogamos con cada una de las nubes privadas, facilitándoles visibilidad, gestión... de una manera mucho más transparente.

¿Qué nuevos controles de seguridad necesita incorporar un CISO en estos entornos?

Sobre todo tiene que entender cuáles son los mecanismos de gestión y de



seguridad en cada uno de los entornos. Debería dialogar con cada uno los proveedores para, antes de contratar un servicio, entender qué mecanismos de seguridad tiene, y si no, poner en marcha algunos mecanismos o mecanismos intermedios, tener un bróker intermedio que les permita hacer esos mecanismos.

Y con todo esto, ¿dónde queda su negocio tradicional?

ADC nos ha dado de comer durante todo este tiempo pero cada vez

más los clientes empiezan a vernos como una empresa que permite dar servicios de aplicación en entornos *multicloud*. Esa transición del entorno ADC tradicional al entorno software y *cloud* no se va a producir de un día para otro pero creemos que en un par de años podemos hacer un balanceo en cuanto a facturación.

¿Cuál va a ser su estrategia para este año?

La idea sería que los clientes que quieren abordar la transformación digital y

quieren mover sus cargas de trabajo a la nube nos ven como un proveedor de servicio de aplicaciones en modo *multicloud*.

Empezar a vender este tipo de servicio a los clientes principales. Hacer acuerdos con las operadoras, sobre todo en el entorno de MSP, ya que vemos que España tiene un tejido industrial de MSP muy grande. Y hacer hincapié en la parte de nuevos modelos de consumo tradicional en la parte de MSP.

¿Cuál es su relación con el CIO y el CISO?

Es una relación que tenemos que mejorar.

Es cierto que nos ven en la parte tradicional porque tienen nuestra tecnología en todos sus entornos. El CISO dice no a cualquier propuesta de seguridad que no esté en su CPD. Ahí tenemos que ir de la mano con brókers o integradores para que vean que trabajar con nosotros les aporta una flexibilidad que hasta ahora no tenían.

¿Qué representa para el mercado y para F5 la adquisición de NGINX?

La aplicación del dato está siendo el principal valor de negocio. Para las empresas que quieren aportar valor en el mundo de la transformación digital, en un entorno *multicloud*, el dato y la aplicación son críticos. Pero la forma en la que se consumen las aplicaciones y los datos ha cambiado. Ahora las empresas consumen los datos y los servicios en la nube. Tienen aplicaciones muy potentes y escalables para crecer. Esa forma de consumir y desarrollar las aplicaciones hace que la gente consuma los datos de una manera activa, bajen las aplicaciones, el código de Internet, lo compile y lo ponga en pre-producción. Y cuando pasa a producción se encarga de imponer la seguridad.

Pero vemos que ya empieza a haber actividades desde el origen de la apli-

cación hasta que se pone en producción. NGINX nos va a permitir cubrir el *gap* entre el momento en el que se desarrolla una aplicación y se pone en producción. Creo que adoptaremos un nivel parecido al de Red Hat donde los clientes consumen los servicios modo *fremium*.

