SD-WAN, ¿cómo garantizar su seguridad?

IDC Analyze the Future

FORCEPOINT POWERED BY Raytheon

Noviembre 2017

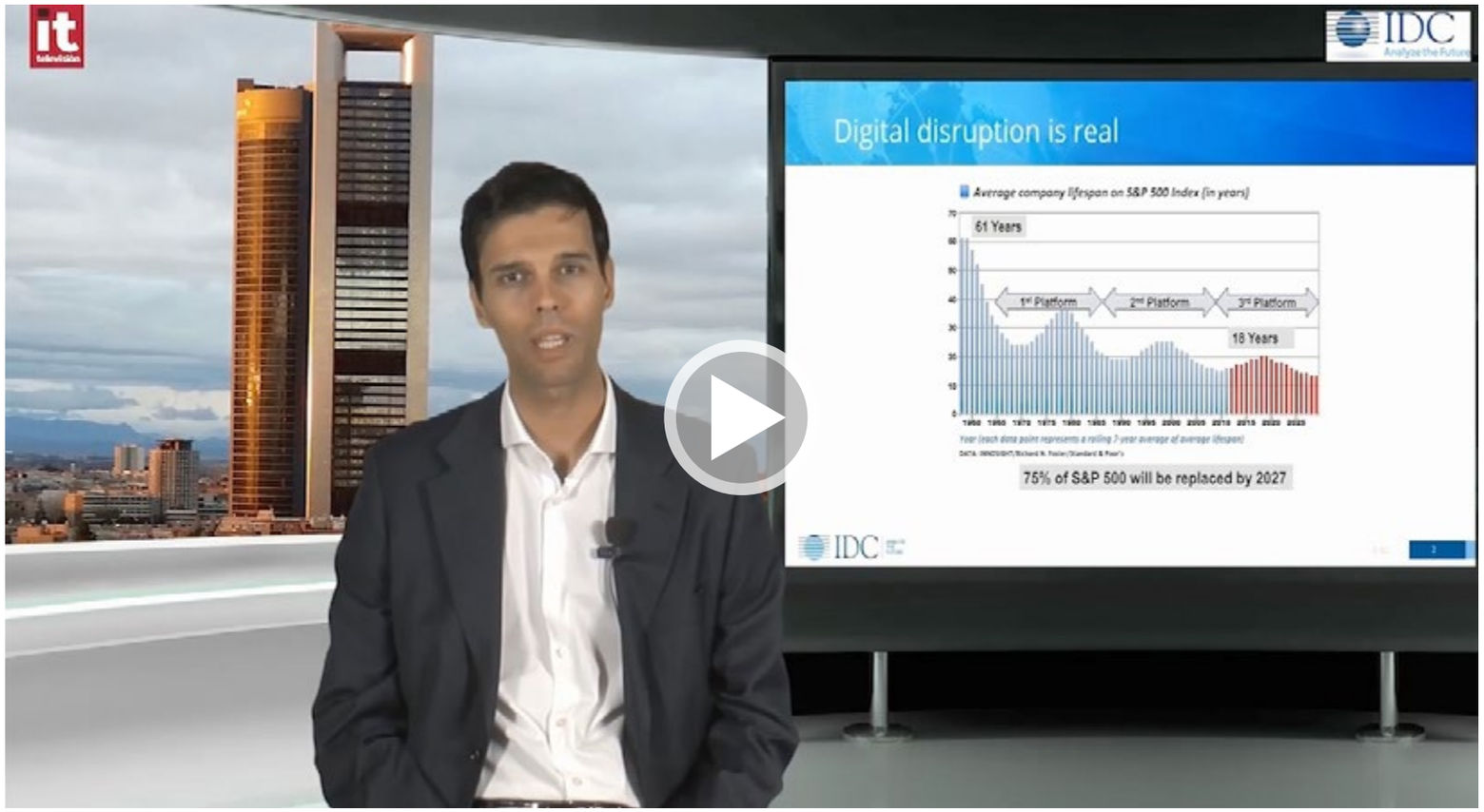
SD-WAN, ¿cómo garantizar su seguridad?

La disponibilidad de las aplicaciones y su rendimiento depende, en buena medida, de la capacidad de la red. La llegada de las redes WAN definidas por software aceleró esa capacidad, pero también se ha abierto una nueva preocupación que no debe desdeñar ninguna empresa que esté pensando en su Transformación Digital, y ésa es la seguridad. Las organizaciones han elevado su conciencia ante esta problemática y buscan seguridad en todas y cada una de las tecnologías que implantan en su organización y no puede ser menos en sus redes SD-WAN.

Los negocios están viendo cómo cambian sus modelos de negocio gracias al uso de tecnologías innovadoras. Hoy, el 92% de las empresas españolas, según una encuesta de IDC, consideran la Transformación Digital como una de las claves de su estrategia.

Dicha transformación pasa por reconsiderar la manera en la que se hacen los negocios, pero también en cómo se ejecutan esos negocios. Las aplicaciones, la conectividad, se han convertido en claves para desarrollar la actividad diaria, y por ello, deben ponerse todos los medios para garantizar a los usuarios, independientemente de dónde se encuentren, que podrán trabajar con sus datos, sus aplicativos de negocio, de forma rápida y segura.

"Es necesario entender las posibilidades de la tercera plataforma: cloud, big data, movilidad y social", explica Ricardo Malhado, Senior Research Analyst de IDC, en el webinar "SD-WAN, ¿cómo garantizar su seguridad?", sesión en la que aseguró que, con ello, "las empresas están pudiendo minimizar el riesgo, aumentar la conectividad, crear nuevos servicios, acceder a infor-



Ricardo Malhado, Senior Analyst en IDC Research, explica el estado del mercado SD-WAN

PINCHA SOBRE LA IMAGEN PARA VER LA SESIÓN

Alfonso Martínez Montero, consulting sales engenieer para EMEA de Forcepoint, detalla las capacidades de la tecnología Multi-Link de Forcepoint

PINCHA SOBRE LA IMAGEN PARA VER LA SESIÓN

mación en tiempo real independientemente de la ubicación, crear productos basados en datos… Y todo ello con el componente social que está cambiando la forma de colaborar, entre empleados y clientes. Es en la tercera plataforma donde está el gasto mundial en TIC, y en los aceleradores de innovación: robótica, IoT, sistemas cognitivos, y realidad aumentada".

Sin embargo, también existen desafíos: "cada pilar de la tercera plataforma es un factor de exposición al riesgo". Según una encuesta de IDC sobre comunicaciones empresariales en la que se preguntó a los participantes cuál es el principal riesgo de TI o red en los próximos dos años, la seguridad fue el más mencionado. "El concepto de perímetro de seguridad ha desaparecido, la superficie de ataque aumenta, crece el número de amenazas que se lanzan a diario. Además, asistimos a la profesionalización del hacking y se ofrece como servicio: criminales que actúan como comunidades open source,

El 21% empresas europeas ya están utilizando SD-WAN y que un 47% planean usarla

comparten las amenazas de forma colaborativa. Es un fenómeno global cada vez más difícil de combatir. Esto cambia la noción de prioridades de las empresas".

Los números de IDC constatan el cambio de prioridades, que se nota en tan solo un año. "En 2016 las prioridades de inversión tecnológica no incluían la seguridad ni la virtualización de la red. En 2017 son preocupaciones dentro del top 5", señala Malhado. La mayor preocupación por la seguridad de la red se debe a un "contexto de urgencia con relación a la necesidad de ser compliance con GDPR, mientras que la inversión en virtualización de la red se debe a que las empresas se están dando cuenta de que las redes son una barrera para alcanzar sus objetivos de negocio. Las empresas quieren innovar, generar nuevos servicios, nuevos modelos de negocio, reducir costes, ser más ágiles. Las redes son cada vez más complejas y caras de monitorizar, también su seguridad es más compleja y difícil de escalar".

Y ante estas necesidades y prioridades de inversión, los presupuestos no se reparten de forma equitativa. Tal y como dijo IDC en la sesión, sí lo hace para Transformación Digital, para migrar a servicios públicos de cloud. Pero todo ello requiere aumentar la conectividad, el ancho de banda y el rendimiento de las aplicaciones críticas que corren por esas redes: "es un acto

"Cuando una compañía está dispuesta a conectar todos sus activos a Internet, tiene que pensar que la seguridad no es una opción, tiene que ser un must" (Forcepoint)

continuo de equilibrismo para dar respuesta a estas necesidades, cuando el presupuesto no crece".

La respuesta tecnológica a estas necesidades es la SD-WAN. Una red de área extensa definida por software; se trata de la evolución de las arquitecturas de red WAN para simplificar el despliegue y gestión de la conectividad entre sedes y oficinas remotas. Ante una "complejidad tecnológica difícil de gestionar, SD-WAN permite separar las funciones", explica Malhado en la sesión web. "Construida sobre redes híbridas, como mínimo, icluye un controlador central y añade una capa de software que permite abstraer esa infraestructura que va debajo y que puede ser MPSL, 4G, Internet… Permite automatizar la configuración de la red y acelera el despliegue".

SD-WAN es una opción que las empresas ya están utilizando ampliamente. Un informe de IDC señala que el 21% empresas europeas ya están utilizando SD-WAN y que un 47% planean usarla. ¿Los motivos? La configuración de la red más ágil, una mayor flexibilidad y capacidad de ancho de banda, optimizar la calidad de servicio, reducir la complejidad de gestión….

Ricardo Malhado, de IDC, y Alfonso Martínez Montero, de Forcepoint, hablando en el webinar sobre los casos de uso de SD-WAN

PINCHA SOBRE LA IMAGEN PARA VER LA SESIÓN

Su adopción es tal, "que el crecimiento del mercado será brutal", destacó Ricardo Malhado, de IDC. "En 2016 fue un mercado de 80 millones de dólares; en 2021 valdrá más de 2.100 millones de dólares, con un CAGR del 92%. La parte de consultoría y gestión tendrán un crecimiento acelerado dada la apurada necesidad de adoptar este tipo de tecnologías. En 2021, los servicios gestionados representarán una opción muy representativa del mercado. Es más que una tendencia, es una realidad a corto plazo".

La omnipresente necesidad de ser seguros

Pero tal y como explicaba Ricardo Malhado al inicio del webinar, la adopción de la tercera plataforma tiene sus riesgos y por ello, la seguridad se ha convertido en una

Alfonso Martínez Montero, consulting sales engenieer para EMEA de Forcepoint, explicó cuál es la propuesta de la compañía para resolver esta necesidad. "La conectividad SD-WAN es el futuro; da igual si es en el perímetro, en cloud, en una oficina remota, VPN, migraciones a cloud o de cloud a sedes. La tecnología Multi-link de Forcepoint es una solución modular que te permite empezar por una sede central y luego ir poniendo en remotas, y de ahí ir al cloud". Entre las capacidades que destacó figuran la eficiencia para conectar ubicaciones, la reducción de costes, la disponibilidad de las aplicaciones, y, sobre todo, la seguridad: "los NSS Labs han destacado nuestros NGF como los mejores".

"Cuando una compañía está dispuesta a conectar todos sus activos a Internet, tiene que pensar que la seguridad no es una opción, tiene que ser un must, estar siempre pendientes de la seguridad. Esa unificación de la gestión de parte de red y la seguridad es una ventaja. Llevamos mucho tiempo en el mercado con la tecnología Multi-link, 15 años, y tenemos muchos clientes

prioridad de inversión para este año. Las SD-WAN ya implican cierta seguridad, pero no es suficiente: "aunque ya tenga encriptación de túneles, no garantiza el acceso a los recursos de Internet. Se necesita más seguridad".

Desde IDC, la recomendación es "aprovechar el paradigma de arquitectura de SD-WAN, de separación de funciones, de gestión centralizada, de escalabilidad, y aplicarlo también a la seguridad y apostar por soluciones que permitan hacer una seguridad gestionada y escalar. Soluciones integradas, como Next Generation Firewall o Unified Threat Management; appliances virtuales o físicas que ganan más funcionalidades y congregan todas las capacidades de seguridad que antes existían individualmente". Se trata de un mercado de gran potencial; de hecho, en España, en el periodo 2016-2021 "el crecimiento de estas tecnologías será de 11,5% al año".

"Recomendamos aprovechar el paradigma de arquitectura de SD-WAN, de separación de funciones, de gestión centralizada, de escalabilidad, y aplicarlo también a la seguridad" (IDC)

que aprovechan sus capacidades", continuó Martínez Montero en su exposición.

Respecto a los casos de uso de esta tecnología, el portavoz de Forcepoint señaló que tienen "clientes que solo necesitan alta disponibilidad en el acceso a internet, tanto en tráfico entrante como saliente. Aportamos la alta disponibilidad independientemente de las líneas y caudales que tengan, podemos balancear el tráfico. La idea es que tengan una mayor capacidad y disponibilidad con SD-WAN. Otros clientes, grandes corporaciones, no solo lo aprovechan para el tráfico que entra y sale hacia cloud, sino que, dada su arquitectura internacional, demandan que les aportemos esa alta disponibilidad de la conectividad entre todas sus sedes. En ese sentido, tenemos varios enlaces hacia sedes, e interconectividad entre todos ellos. Siempre con la palabra SD-WAN y la seguridad por delante. Además, también podemos incluir otra serie de seguridad como CASB para aportar un mayor nivel de protección".

Por último, IDC señaló una predicción y una recomendación sobre este tipo de soluciones. "La virtualización se convertirá en la norma, dejaremos lo físico y pasaremos a lo virtual, hablaremos de la virtualización de firewalls, etc... Además, vemos que el open source será una forma de desarrollar nuevos servicios, y la razón para adoptarlo será no tanto bajar el coste del desarrollo y mantenimiento de la tecnología, sino la capacidad de desarrollar servicios más rápidamente. Y esta virtualización de funciones de red, llevará retos de orquestación de servicios".

En cuanto a la recomendación de la consultora, Malhado dijo que "las empresas no deben intentar locuras. Deben aprovechar al máximo la infraestructura existente y construir el overlay de SD-WAN por encima e ir incorporando los casos de uso por encima. Aprovechar el paradigma de arquitectura de SD-WAN: gestión centralizada de la red, e implementar soluciones de seguridad que permitan también una gestión centralizada de la seguridad de la red y escalar con la red SD-WAN".

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn

Enlaces relacionados

- V SD-WAN, ¿cómo garantizar su seguridad?
- W Presentación IDC: SD-WAN: Mercado y retos
- W Presentación Forcepoint: SD-WAN y Transformación Digital
- W Informe Computing Research: Asegurando el sueño digital