Hibridez, pago por uso y seguridad;
tridente obligatorio en el puesto de trabajo

Mucho ha cambiado la manera en la que las empresas conciben el puesto de trabajo. Lo híbrido marca el paso de la inversión en este crítico entorno, lo que exige la adopción de modelos flexibles, basados en el pago por uso, que permitan a los empleados disfrutar de la máxima agilidad, simplicidad y transparencia en el uso de la tecnología. Y en un entorno completamente seguro. Un panorama en el que el canal es protagonista. Para llamar la atención sobre las oportunidades en este entorno, Ingram Micro reunió a su canal en Madrid en una jornada en la que contó con la participación de Citrix, HPE y Sonicwall.

Marilés de Pedro

Martín Trullás, director del área de Advanced Solutions de Ingram Micro, aseguró que los modelos de pago por uso están cobrando más relevancia en estos entornos híbridos. "Tanto clientes como fabricantes están apostando por estas fórmulas". Los proyectos de nube híbrida son una realidad. "No solo los hiperescalares son protagonistas en estos despliegues. También los fabricantes están trabajando en sus propios modelos de *cloud* híbrida".

Programa CSP de Citrix

"El modelo CSP (Citrix Service Provider) todavía es un gran desconocido para el canal". Antonio Zamora, Citrix *business manager* en Ingram Micro, reconoce que la enorme oportunidad que supone la implantación de un modelo de pago por uso todavía no ha sido detectada en su totalidad por los *partners* españoles. "En Europa crece de manera exponencial a un ritmo mucho más elevado que los modelos tradicionales, con regiones, como los Países Bajos, por ejemplo, con el 70 % de los ingresos de Citrix generados por él". En España, sin embargo, el ascenso está costando más, con crecimientos "similares a los que exhibe la venta tradicional".

El modelo CSP de Citrix, completamente flexible, apela a una manera sencilla de desplegar entornos híbridos, ya sea en las instalaciones del cliente o en la nube. "En el despliegue de un espacio de trabajo digital las empresas deben observar el perfil de sus trabajadores, permitiendo que desarrollen su labor desde cualquier lugar, con cualquier dispositivo y con las aplicaciones que necesitan para ella. En un entorno completamente seguro", recordó Carlos Lacuna, Citrix CSP *manager*.

El programa CSP de Citrix permite a los proveedores de servicio desplegar sus servicios "en un modelo de pago por uso, con precios estables, a mes vencido y sólo por lo que ha consumido la empresa". Este tipo de *partners* puede acceder a los servicios técnicos

El programa CSP de Citrix permite a los proveedores de servicio desplegar sus servicios en un modelo de pago por uso, con precios estables, a mes vencido y sólo por lo que ha consumido la empresa

de Citrix y disfrutan de una política flexible de licencias en función de las necesidades de sus clientes (que incluye licencias para realizar pruebas, entornos de test y demostraciones y también para su uso interno). Además se incluye una batería de recursos que incluye iniciativas de marketing, formación y soporte. Los *partners* pueden acceder a Partner Central, que cuenta con un gran caudal de información útil; a Citrix Education, donde se ubica el panel completo de certificaciones y la plataforma de *elearning*; a SalesIQ_, un repositorio de información muy completo que incluye, por ejemplo, arquitecturas de referencia, campañas de marketing a disposición de los *partners*, ventajas competitivas de Citrix, etc.; y a ECC Enablement, con cursos de formación y anuncios de seminarios.

El programa cuenta con 3 niveles (Member, Prefereed y Premier), diferenciados en función de su nivel de certificación, formación y nivel de facturación. En función de la solución que el *partner* quiera desplegar deberá contar con alguna de las certificaciones del programa: virtualización, cloud (hay una conjunta para ambas) o las específicas para el resto de la oferta de Citrix. "Cuanta más formación y certificaciones consiga, más posibilidad tendrá el *partner* de desplegar proyectos de mayor valor".

Para llevar a cabo los proyectos, el modelo

permite dos formas de trabajar. Una, tradicional, en la que el proveedor de servicio diseña completamente la solución y es único responsable de su implantación, gestión y despliegue; y otra, que apela a un modelo en la nube, que proporciona una capa de gestión para controlar el servicio que concede el proveedor a su cliente (este modelo debe tener un mínimo de 25 usuarios).

Lacuna apeló a la posibilidad que ofrecen los modelos CSP de diferenciar entre entornos *multi-tenant* y *single-tenant*. "El modelo CSP permite contar con un único panel de control para varios clientes, cada uno con su acceso independiente, pero también es posible ofrecer la opción tradicional de Citrix, que permite que un único panel sirva para gestionar a un único cliente".

El directivo de Citrix recordó el valor de la herramienta LUI (License Usage Insights), que proporciona información sobre los usuarios que incluye la plataforma de virtualización y las tendencias de uso. Es un servicio basado en *cloud*, en el que se da visibilidad a lo que está en el entorno de la nube y lo que se aloja en un entorno *onpremise*.

El valor de HPE GreenLake para el canal

HPE GreenLake llena un hueco muy importante en la forma en la que las empresas consumen la nube. Teniendo en cuenta que en la actualidad en torno al 70 % de las aplicaciones siguen residiendo fuera de la nube, por temas de cumplimiento, seguridad, rendimiento y otros factores; es absolutamente relevante observar qué tipo de información y qué tipo de aplicaciones son susceptibles de que puedan alojarse fuera de los entornos privados y cuáles no.

Por tanto, las empresas exigen nuevas fórmulas para trasladar, a sus centros de datos, la experiencia de la nube moderna. "HPE GreenLake ofrece, tanto a clientes como a los *partners* esta experiencia, independientemente de la carga, de la aplicación, del tipo de proyecto desplegado o del entorno, sea en un *colocation*, en el *edge* o en un centro de datos privado", explicó Ángel D. López, HPE GreenLake *senior sales manager* en Ingram Micro. Una experiencia, absolutamente flexible, bajo un modelo de

pago por uso, totalmente gestionado y sobre el que las empresas tienen un control absoluto. "Se paga solo por lo que se consume. No se penalizan los "picos". Es posible, gracias a la flexibilidad que aporta, crecer o decrecer en el gasto según las necesidades".

López repasó las últimas novedades incorporadas a esta plataforma el pasado mes de junio con nuevas posibilidades de hibridez con los principales hiperescalares. En el área de la infraestructura, se ha incorporado prácticamente toda la oferta de HPE (cómputo, almacenamiento y red), lo que permite acercarse a los clientes con una oferta completa, con una potente propuesta tecnológica. "Se han potenciado las capacidades de seguridad y de cumplimiento normativo ya que una gran parte de las cargas que no se pueden elevar a la nube son por la posible vulnerabilidad del dato y el cumplimiento",

> HPE GreenLake ofrece un experiencia de nube, independientemente de la carga, de la aplicación, del tipo de proyecto desplegado o del entorno

recordó. "El dato queda alojado en el centro de datos".

Claves los servicios, "tanto los financieros, piedra angular, como también los que apelan a la consultoría para ayudar al *partner* en su acercamiento a los clientes e incluso servicios complementarios en la gestión de la plataforma".

López insistió en la gestión intuitiva que permite HPE GreenLake, muy similar a la que tienen los principales hiperescalares, "con capacidades de autoaprovisionamiento y

entornos para que los desarrolladores puedan crear contenedores". El área en el que más se está invirtiendo es en los casos de uso, con un completo *marketplace* y un elenco de ISV con el que se colabora (VMware, Microsoft, Red Hat o SuSE, entre otros).

En el entorno del puesto de trabajo HPE GreenLake se torna en una "propuesta de infraestructura muy válida para el despliegue de proyectos de VDI". López recordó su alianza con Citrix en este apartado. "Aseguramos que los datos estén centralizados, en un entorno *onpremise* y en la geografía de los clientes, con más seguridad ya que no se lleva ninguna información confidencial a la nube", recordó. "Conseguimos una reducción de costes, con una enorme flexibilidad financiera".

El directivo de Ingram Micro insistió en el carácter global de esta plataforma, con una oferta integral, que ofrece múltiples sabores tecnológicos en el área de la virtualización del puesto de trabajo. "El control que permite, sencillo, supera el tradicional obstáculo que experimentan los usuarios en las subidas de sus cargas a la nube". Y también en temas de rendimiento y latencia. "Al llevar un VDI a un hiperescalar el usuario se encuentra con distancias importantes entre dónde se presenta el dato y dónde se aloja. Es esencial acercar estos escritorios y puestos de trabajo al centro de datos, al origen del que beben".

La seguridad, esencial en el puesto de trabajo

La seguridad se torna elemento básico en este entorno del puesto de trabajo. Sergio Martínez, director general de Sonicwall en España y Portugal, recuerda la complejidad de un panorama en el que, a pesar de descender el número de ataques en los pasados meses, éstos se han vuelto mucho más sofisticados y dirigidos. "Las amenazas encriptadas han crecido de forma exponencial en los últimos seis meses. Más del 70 % del tráfico en Internet es encriptado, lo que supone una avenida para el cibercrimen". Nadie inspecciona ese tráfico y el *firewall*, por

el que transcurre, pieza esencial, no es suficiente para armar una adecuada protección. "Además, aparecen muchas más tecnologías que dificultan la función que desempeña el *firewall*: DNS sobre HTTPS, el uso intensivo de UDP, etc.", relató.

Martínez insistió, por tanto, en la imprescindible alianza del *firewall* con el "otro lado, que es el *endpoint*, para que sea posible inspeccionar el tráfico; tarea básica para garantizar una adecuada protección". Un complejo panorama al que se suma el crecimiento de *malware* desconocido, lo que exige, no una seguridad basada en patrones sino en un análisis del comportamiento. "Los *hackers* están poniendo mucho foco también en el robo de credenciales, que es la nueva pandemia", completó.

Para hacer frente a este complejo panorama, Sonicwall despliega su negocio en tres áreas: despliegue de nuevos *endpoints*, control y visibilidad de la red con el *firewall* y una tecnología accesible a las pymes.

> "Es imprescindible establecer una alianza entre *firewall* y *endpoint*, para que sea posible inspeccionar el tráfico; tarea básica para garantizar una adecuada protección"

Álvaro de Pedro, Sonicwall *business developer manager* de Ingram Micro, insistió en que la oferta de la marca transcurre mucho más allá del *firewall*. "Junto a su foco en la seguridad perimetral despliega soluciones de protección en el puesto de trabajo". De Pedro recordó que hay mucho por hacer en materia de seguridad. "Las empresas están cada vez más distribuidas, con empleados

dispersos. El centro de la empresa debe ser el usuario y es esencial la manera en la que actúa con los recursos de la misma".

En el entorno del puesto de trabajo, Sonicwall cuenta con soluciones basadas en inteligencia artificial que analizan lo que está ocurriendo en tiempo real, protegiendo tanto el correo y las aplicaciones que están en la nube como el propio entorno; lo que incluye soluciones Zero Trust.

En esta oferta se incluye una solución CASB, Cloud App Security, que, entre otras funciones, realiza un análisis, en tiempo real, de las amenazas antes de que lleguen al *firewall* o al *endpoint* y detecta los ataques a Microsoft 365 o Google Suite. "No está basada en firmas sino en comportamientos", recordó. No se compromete el rendimiento y, haciendo uso de la consola que integra la solución, es posible controlar los accesos a la nube, de una manera granular, observando quién está accediendo y a qué cargas, lo que ayuda al cumplimiento normativo. "En el área de la protección de datos, es posible definir qué datos se alojan en la nube".

La otra solución es Capture Client Powered by Sentinel. "Se trata de una vuelta completa al antivirus tradicional, con un motor dinámico que analiza qué ocurre en el *endpoint* en todo momento: URL, dispositivos, conexiones, etc.", calificó. Es una solución que minimiza cualquier tipo de amenaza, sobre todo en entornos fuera de la oficina, con funcionalidades de EDR e inspección del tráfico cifrado, y todo ello "en una única consola centralizada".

Por último, en el área de Zero Trust, la apuesta lleva el nombre de Sonicwall Cloud Edge Secure Access, que proporciona acceso remoto seguro, verificando al usuario y al contexto, con una segmentación de la confianza en función del rango del empleado.