

Virtualización y enterprise browser: cuando competir no impide convivir

ciberseguridadTIC

Virtualización y enterprise browser: cuando competir no impide convivir

El puesto de trabajo se ha convertido en uno de los escenarios en los que más claramente confluyen los cambios tecnológicos de los últimos años. El trabajo híbrido, el uso de dispositivos personales y, sobre todo, el creciente peso de las aplicaciones SaaS y web están obligando a las empresas a replantearse cómo proporcionar un acceso seguro a aplicaciones y datos.

Durante años, la virtualización del puesto de trabajo ha sido una de las principales respuestas a este reto, centralizando aplicaciones, escritorios y datos para mantener el control independientemente del dispositivo desde el que se conecte el usuario. Ahora gana protagonismo otra aproximación: el navegador corporativo o enterprise browser, que busca convertir



una herramienta que ya utilizan prácticamente todos los empleados en un entorno de acceso protegido.

¿Estamos ante dos modelos que compiten por resolver el mismo problema? ¿Puede el navegador sustituir a la virtualización en determina-

dos escenarios? ¿O tiene más sentido pensar en ellos como tecnologías complementarias? Para analizar qué aporta cada aproximación y dónde encaja cada una, reunimos a Fernando Feliu, Executive Managing Director de Virtual Cable, y Eusebio Nieva, Security Evangelist de Check Point.

Dos aproximaciones a un mismo problema

Para Eusebio Nieva, el punto de partida del enterprise browser está en un cambio muy concreto: el navegador se ha convertido en “la herramienta ubicua de acceso a las aplicaciones”. El responsable de Check Point estima que prácticamente todas las aplicaciones disponen ya de algún tipo de interfaz web, lo que permite utilizar el navegador como punto desde el que controlar y proteger tanto el acceso de los empleados a Internet como el acceso remoto a las aplicaciones corporativas.

La propuesta consiste en añadir sobre un navegador basado en motores estándar distintas capas de protección, cifrado y control. Una de



“El navegador es la herramienta ubicua de acceso a las aplicaciones”

Eusebio Nieva,
Security Evangelist de Check Point

sus ventajas, explica Nieva, es que el usuario continúa trabajando con una herramienta que ya conoce, “sin necesidad de hacer un despliegue enorme de nuevas tecnologías y tampoco sin necesidad de enseñar a los usuarios”.

La virtualización parte de una filosofía diferente. Fernando Feliu recuerda que las empresas no

Tecnologías frente a frente

viven exclusivamente en un mundo web. Siguen existiendo aplicaciones legacy, infraestructuras on-premise y entornos híbridos en los que el usuario necesita algo más que acceder a una determinada aplicación desde un navegador.

En estos casos, la virtualización permite proporcionar “un escritorio completo” y controlar desde un punto central qué aplicaciones, datos y recursos puede utilizar cada persona. El procesamiento y la información permanecen en la infraestructura corporativa y son independientes del dispositivo desde el que se accede. “El planteamiento es muy parecido, lo que pasa es que desde un punto de vista también muy diferente”, resume Feliu.

La simplificación impulsa al navegador

Si hay un argumento que Nieva repite al explicar el auge del navegador corporativo es la simplificación. Cuantas más aplicaciones pasan a disponer de una interfaz web, menor puede ser el número de componentes intermedios necesarios para llegar hasta ellas.

“Todo aquello que puedas hacer con una única herramienta que sea fácilmente adaptable por los usuarios” facilita su adopción, señala. Sobre esa herramienta pueden incorporarse mecanismos de autorización, cifrado y seguridad sin modificar sustancialmente la forma de trabajar del empleado.

También se reduce, en determinados escenarios, la superficie tecnológica que debe mantenerse. Si el acceso puede resolverse directamente mediante el navegador, explica Nieva, la empresa evita tener que gestionar y parchear algunos sistemas operativos o componentes intermedios. “Si puedes adaptarte a ese caso de uso, obviamente eso es más sencillo de adoptar por parte de las empresas”.

Feliu introduce aquí un matiz importante. Esa simplificación resulta válida cuando el navegador puede resolver el caso de uso, pero no todas las organizaciones ni todos los puestos de trabajo tienen las mismas necesidades. La virtualización permite entregar una aplicación concreta, un conjunto de aplicaciones o un es-



“La virtualización es como si tuvieras dentro de tu pantalla una mirilla que ve lo que está sucediendo en otro sitio”

Fernando Feliu,
Executive Managing Director de **Virtual Cable**

critorio completo y aplicar sobre ellos políticas diferentes de acceso.

Por eso prefiere no plantear ambas opciones como excluyentes. “No son tecnologías alternativas, pueden ser tecnologías complemen-

Tecnologías frente a frente

tarias”. Desde la virtualización, añade, pueden definirse políticas de autenticación multifactor, limitar el uso de USB o impresoras y establecer quién accede a una aplicación, desde dónde y durante cuánto tiempo.

Dos maneras de abordar la seguridad

Las diferencias se hacen más visibles cuando la conversación se traslada a la ciberseguridad. En el modelo que defiende Check Point, una de las ventajas consiste precisamente en acortar la cadena entre usuario y aplicación siempre que la arquitectura lo permita.

El navegador corporativo puede comprobar el dispositivo desde el que se produce la conexión, gestionar la autorización, proteger las comunicaciones y establecer qué puede hacer el usuario con los datos. “Cuanto más simple sea el acceso”, menos piezas intermedias habrá que administrar y proteger, sostiene Eusebio Nieva, reconociendo que eso no significa que pueda utilizarse en cualquier situación y que hay aplicaciones que no pueden trasla-

darse fácilmente a un entorno web. Cuando esto ocurre, “tienes que ir a métodos híbridos, obviamente, métodos en los cuales convivan ambos mundos”.

La virtualización busca aislar el dispositivo del entorno en el que realmente se ejecutan las aplicaciones y permanecen los datos. Fernando Feliu lo explica con una imagen sencilla: es “como si tú tuvieras dentro de tu pantalla una mirilla que ve lo que está sucediendo en otro sitio”. El usuario recibe la representación de lo que se está ejecutando en la infraestructura remota, mientras la computación y los datos permanecen en ese entorno controlado.

A ello se suma la gestión centralizada. Perfiles, aplicaciones, permisos y sesiones pueden administrarse desde un mismo punto, algo que el directivo de Virtual Cable considera especialmente relevante a medida que los puestos de trabajo se vuelven más cambiantes. “Hay que tener un control muy exhaustivo también de a qué datos se tiene acceso, quién, dónde y cuándo”.



BYOD: uno de los terrenos donde se cruzan

El acceso desde dispositivos no corporativos muestra bien tanto las coincidencias como las diferencias entre ambos modelos.

Nieva identifica precisamente el BYOD y el acceso remoto como uno de los “puntos dulces” actuales del enterprise browser. Un empleado

o un tercero puede utilizar un dispositivo que no pertenece a la organización para entrar en las aplicaciones autorizadas mediante el perfil corporativo del navegador. La empresa puede verificar las condiciones de seguridad del equipo y controlar qué ocurre con la información, por ejemplo, evitando que determinados



datos permanezcan almacenados localmente. El límite vuelve a aparecer cuando el usuario necesita un escritorio completo o aplicaciones que no funcionan en un entorno web. Eusebio Nieva lo reconoce: “No es el escenario óptimo para el navegador”. En cambio, cuando el objetivo es acceder a aplicaciones y datos con interfaz web, considera que puede hacerse de una manera mucho más directa.

Fernando Feliu, por su parte, defiende otra forma de independizar el acceso del dispositivo. Con la

virtualización, señala, el usuario puede conectarse desde un navegador convencional sin que los datos tengan que residir en ese equipo. Y amplía los casos de uso más allá del trabajo remoto: administraciones públicas, hospitales, logística, industria o grandes organizaciones distribuidas en distintas ubicaciones.

En estos escenarios, más que el tamaño de la empresa, lo determinante es la necesidad de centralizar la gestión o de utilizar aplicaciones y capacidades que no pueden reducirse al navegador.

Tecnologías frente a frente

¿Qué debe valorar una empresa?

La diferencia de filosofía vuelve a aparecer al analizar qué debería tener en cuenta una organización antes de apostar por una u otra tecnología. Pone el foco el directivo de Check Point Software en la arquitectura existente y en el número de componentes necesarios para proporcionar el acceso. El navegador corporativo puede trasladar una parte de los controles desde el propio puesto de trabajo hacia la forma en que se accede a las aplicaciones. “Puedes tener menos controles en el puesto de trabajo y poner más controles en la forma de acceder”, explica Eusebio Nieva.

La virtualización, por su parte, cobra sentido cuando la organización quiere mantener centralizados no solo los controles de acceso, sino también la ejecución de las aplicaciones y los datos. Esto permite asignar a cada usuario sus aplicaciones, sesiones y recursos y mantener actualizados esos entornos desde un único punto. Feliu vuelve a insistir en esa idea de control: si una empresa quiere que “la actualización de

“Todo aquello que puedas hacer con una única herramienta que sea fácilmente adaptable por los usuarios facilita la adopción”

Eusebio Nieva,
Security Evangelist de **Check Point**

todas las aplicaciones esté al día en todos los puestos de trabajo” y gestionar de forma centralizada cuándo se abren y cierran las sesiones, la virtualización ofrece ese modelo. “Pero vuelvo a decir que no es excluyente una cosa de otra”.

La IA añade una nueva variable

La inteligencia artificial introduce además nuevas presiones sobre ambos modelos. Para Eusebio Nieva, su impacto sobre el navegador corporativo es indirecto, pero importante. La IA está acelerando el descubrimiento y explota-

ción de vulnerabilidades y, con ello, aumentando la presión sobre los equipos de seguridad para mantener actualizados sus sistemas.

En ese contexto, reducir el número de componentes que hay que gestionar puede convertirse en una ventaja. “Al tener menos piezas que parchear”, argumenta, se simplifica parte del trabajo de los equipos de seguridad. No es tanto que la IA cambie por sí misma la forma de acceso como que acelera la necesidad de reducir complejidad.

Fernando Feliu observa otro riesgo: la aparición del Bring Your Own AI, con empleados que utilizan o desarrollan sus propios agentes sin el control de la organización y que pueden terminar trabajando con información corporativa.

La respuesta, desde su perspectiva, vuelve a pasar por la centralización: “Asignar los agentes y realmente asignar los datos que pueden utilizar esos agentes dentro de la corporación” permite establecer qué herramientas de IA puede utilizar cada usuario y a qué información pueden acceder.

Tecnologías frente a frente

“Si quieres entornos complejos, un mayor control sobre el dato y una gestión mucho más centralizada, entonces tienes que ir a la virtualización”

Fernando Feliu,
Executive Managing Director de **Virtual Cable**

¿Competencia o convivencia?

Llegados a este punto, ninguno de los dos niega que exista cierto solapamiento. “Está claro que tienen cierta competencia”, admite Nieva. Hay casos de uso que pueden resolverse con cualquiera de las dos aproximaciones y otros en los que las diferencias son mucho más claras. Incluso dentro de un escritorio virtualizado puede utilizarse un navegador corporativo. “Hay casos de uso claros en los cuales están compitiendo, pero hay otros en los que no tienen por



qué competir”, explica el responsable de Check Point. Su conclusión es clara: “Yo creo que ambos pueden convivir. Es cierto que compiten, es que no podemos negar la evidencia”.

Fernando Feliu coincide en la convivencia, aunque sitúa la virtualización como la opción más adecuada cuando aparecen entornos complejos, aplicaciones no web, necesidades de computación elevadas o ficheros pesados asociados, por ejemplo, a arquitectura, diseño industrial o imagen médica.

El navegador corporativo encuentra, a su juicio,

un espacio claro cuando las aplicaciones son web y el navegador puede convertirse en el principal entorno de trabajo. Cuando las necesidades van más allá, sostiene que la virtualización ofrece más posibilidades.

Empezar por el caso de uso, no por la tecnología

La última cuestión termina acercando más las posiciones de lo que podría sugerir inicialmente un debate entre virtualización y navegador corporativo.

Tecnologías frente a frente

Para Eusebio Nieva, la primera pregunta de un CIO o un CISO debería ser muy sencilla: “¿Qué quieres resolver?”. No es lo mismo proporcionar acceso remoto a terceros que a empleados, trabajar exclusivamente con aplicaciones web o necesitar escritorios completos. Una vez identificado el caso de uso, habrá que comparar las ventajas e inconvenientes de cada alternativa.

Antes de escoger una tecnología, una organización debe saber “qué tiene y qué quiere tener en el futuro”, coincide Fernando Feliu, quien añade que una advertencia que sirve también para cerrar el debate: “Las tecnologías no se implantan por modas ni se implantan por tendencias”.

Arquitectura, gestión, mantenimiento, experiencia de usuario, seguridad, presupuesto y evolución futura deben formar parte de la decisión. Y esa decisión no tiene necesariamente que desembocar en un único modelo. La propia conversación entre ambos muestra que, a medida que el puesto de trabajo se hace más heterogéneo, la frontera entre virtualización y navegador corporativo puede ser menos rígida de lo que parece. 