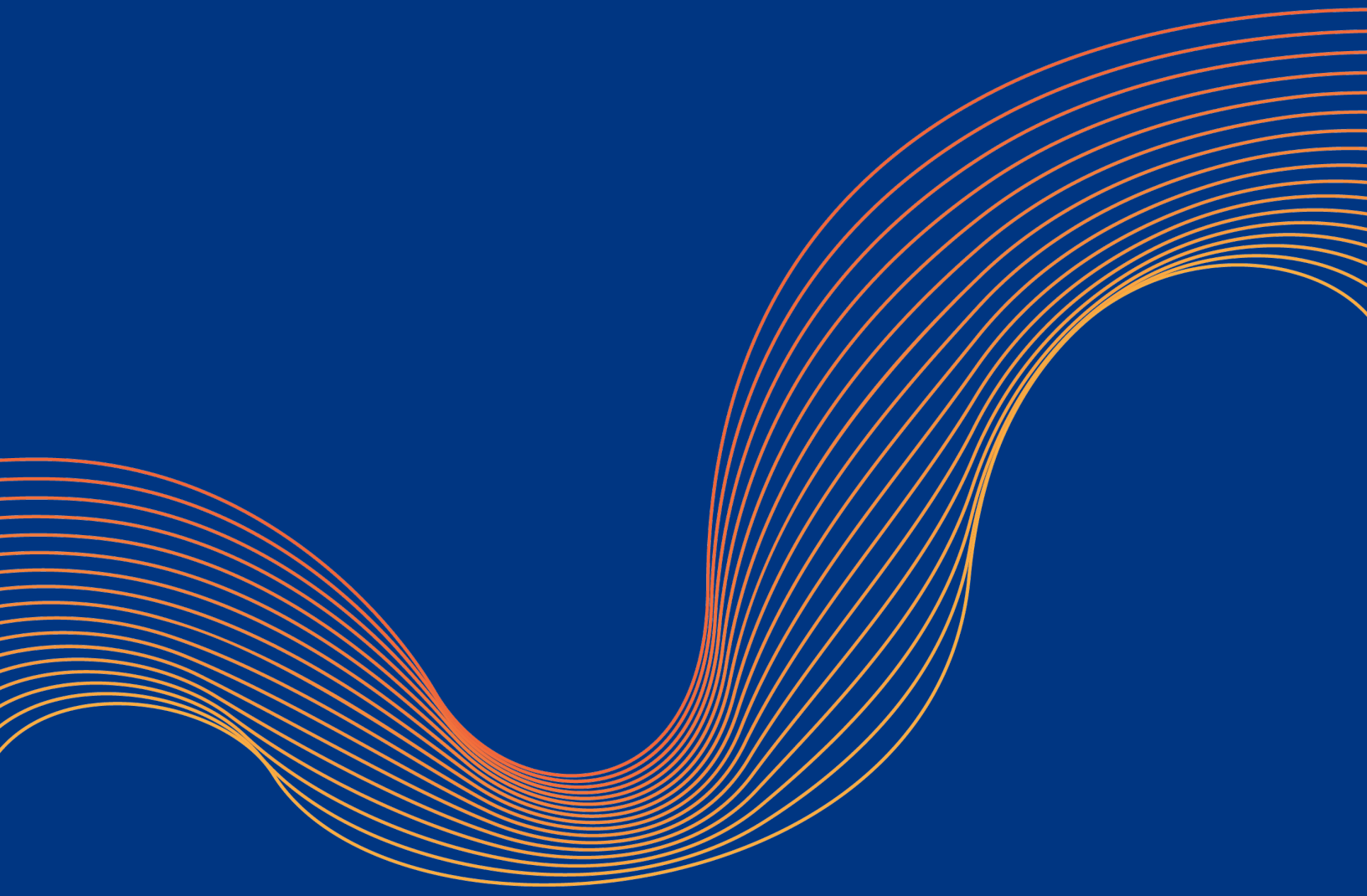
CLOUDFLARE

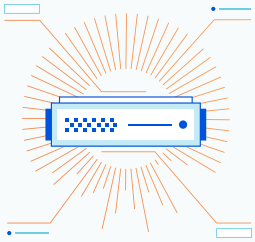
Desafíos comunes del aislamiento del navegador y cómo superarlos

La encrucijada de la navegación por Internet y la seguridad Zero Trust



+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

ÍNDICE



Introducción

Los equipos de TI y seguridad tienen buenas razones para no confiar en la red pública. El phishing y el malware representaron el 39 % de todas las fugas de datos en 2020, según reveló un informe de Verizon. Además, un estudio de Forrester Consulting encargado por Cloudflare concluyó que en 2020, el 61 % de las empresas con más de 1 000 empleados experimentaron un aumento en los ataques de phishing en comparación con años anteriores.

Todos los profesionales de TI y seguridad quieren evitar que su organización forme parte de estas estadísticas. En concreto, buscan:

- **Bloquear el malware y el phishing,** que cambian constantemente de táctica para burlar las medidas de detección.
- **Evitar la pérdida de datos en general,** ya sea a través de dispositivos infectados o interacciones de usuario.
- **Conseguir mejor visibilidad de la navegación por Internet de los empleados,** para comprender el panorama de amenazas específico de su organización y responder más rápidamente a las filtraciones que se produzcan.

Estos casos de uso son elementos importantes de la **seguridad Zero Trust**, que no debe confiar implícitamente en las propiedades y el código de Internet, de ahí que deban procesarse de forma segura en el momento de la interacción con el usuario.

Para lograr estos objetivos, algunas organizaciones están recurriendo al aislamiento del navegador, una estrategia en la que la navegación de los empleados por Internet se mantiene aislada de las redes e infraestructuras locales. Aplicado de forma exhaustiva y eficiente, el aislamiento del navegador muestra potencial para ser la forma más eficaz de mitigar los ataques procedentes de Internet. Lamentablemente, hasta ahora ha sido una tecnología de nicho debido a una serie de desafíos relativos al **coste elevado, experiencias de navegación poco satisfactorias, obstáculos en la gestión logística** y **vulnerabilidades de seguridad.**

Este documento describe esos desafíos en detalle para ayudar a los equipos de seguridad y TI a comprender mejor sus necesidades de seguridad de navegación por Internet. También define un método para superar estos retos y, por último, explica cómo Cloudflare ha integrado este enfoque en su red global.

Desafíos de las estrategias comunes para mitigar los problemas del aislamiento del navegador

El malware, el phishing y la pérdida de datos afectan a las organizaciones de todos los sectores y actividades. El aislamiento del navegador es la solución más usada para abordar los dos primeros tipos de amenazas, ya que refuerza la lista de bloqueo, la comparación de archivos y los enfoques de comportamiento utilizados por las puertas de enlace web seguras.

En la práctica, sin embargo, el aislamiento del navegador a menudo no consigue este objetivo.

¿Por qué razón? Piensa en las limitaciones de los métodos de aislamiento de navegadores más comunes:

Transmisión de capturas de pantalla de la actividad de navegación desde la nube

Este enfoque, que a veces se denomina "inserción de píxeles", captura eventos en el navegador del usuario final y los transmite a un navegador remoto alojado en la nube, que realiza acciones de navegación y transmite una secuencia de imágenes de píxeles de la ventana del navegador remoto de vuelta al usuario final. De esta manera, cualquier código malicioso, ya sea por una descarga automática o una acción intencionada del usuario, se mantiene aislado del dispositivo del usuario final. Además, los sitios potenciales de phishing, como las páginas con campos de formulario de nombre de usuario/contraseña, pueden mostrarse en modo de solo lectura o con un mensaje de advertencia añadido.

Este enfoque hace un buen trabajo aislando los dispositivos de punto de conexión del malware y el phishing. Sin embargo, plantea varios problemas como:

Latencia del usuario final: cuando el aislamiento remoto del navegador se aloja en la nube pública (o en una red privada limitada geográficamente), los usuarios finales pueden experimentar latencia cuando están físicamente distantes de los centros de datos de aislamiento del navegador. Este problema se agrava cuando el tráfico del usuario final pasa por otras herramientas de seguridad como una puerta de enlace web segura, que no están alojadas en los mismos centros de datos, o que necesitan "pasar" repetidas veces a través de contenedores con arquitectura ineficiente.

Costes elevados: la codificación constante de la transmisión de vídeo de páginas web remotas a dispositivos de punto de conexión de los usuarios finales es muy cara desde el punto de vista computacional. También requiere un ancho de banda considerable, incluso cuando se optimizan mucho. Estos costes se suelen reflejar en los clientes.

Vulnerabilidades de seguridad: dado que la "inserción de píxeles" a menudo causa experiencias de usuario final no satisfactorias, muchas organizaciones solo requieren su uso en equipos con acceso a datos especialmente confidenciales, como finanzas, recursos humanos o ejecutivos de la empresa. La organización también puede aplicar la navegación remota solo a un pequeño porcentaje de páginas web consideradas especialmente poco seguras. De cualquier manera, la organización permanecerá expuesta, ya sea a causa de empleados sin protección o por culpa de sitios "fiables" que se han visto comprometidos.

Altos requisitos de ancho de banda: la transmisión de imágenes requiere mucha capacidad de ancho de banda, lo que puede sobrecargar la infraestructura de red y afectar negativamente la experiencia del usuario final. Además, la densidad de píxeles aumenta exponencialmente con la resolución, lo que significa que las sesiones remotas del navegador (en particular las fuentes) en los dispositivos HiDPI pueden parecer borrosas o desenfocadas.

Descomposición de sitios web en la nube y eliminación del código malicioso

Este método se conoce a menudo como manipulación del DOM. En la programación de un navegador web, el DOM, o modelo de objetos del documento, es la representación de datos de los objetos que componen la estructura y el contenido de una página web. En la manipulación del DOM, un navegador remoto alojado en la nube examina el HTML, el CSS y otros elementos de una página web, e intenta eliminar el código activo como Javascript, las vulnerabilidades conocidas y otros contenidos potencialmente maliciosos. El navegador remoto reenvía este código al navegador del usuario final, que lo utiliza para reconstruir una versión "limpia" de la página. Además, como en la "inserción de píxeles", la manipulación del DOM también puede marcar ciertas páginas como riesgos de phishing.

Dado que la manipulación del DOM solo transfiere el código del sitio web, en lugar de una transmisión completa de la experiencia de navegación, requiere menos ancho de banda y puede acelerar las experiencias del usuario final.

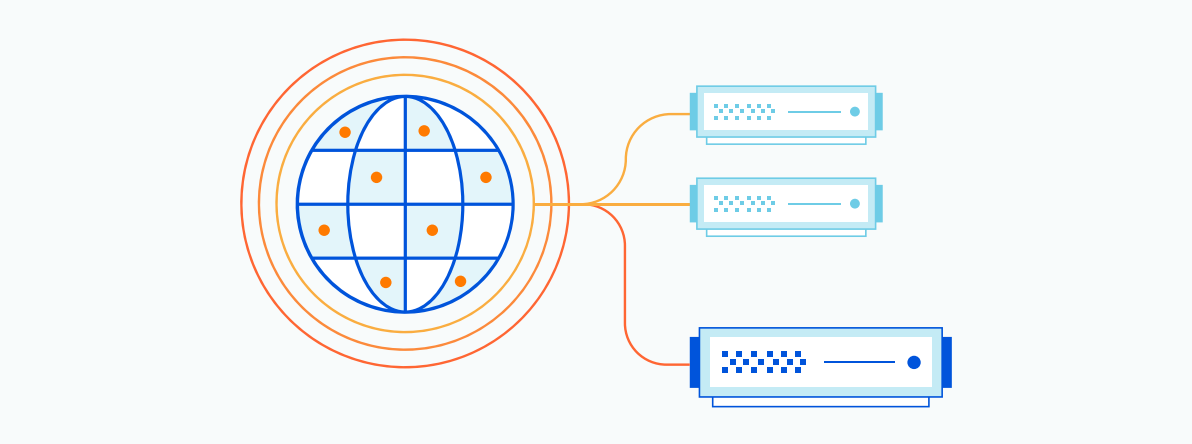
Sin embargo, presenta problemas como:

Latencia del usuario final: al igual que con la "inserción de píxeles", si el aislamiento del navegador de manipulación del DOM funciona en la nube pública (o en una red privada limitada geográficamente), los usuarios finales pueden experimentar latencia cuando los servidores de origen están demasiado lejos, o cuando el aislamiento del navegador y otras herramientas de seguridad están alojadas en diferentes centros de datos.

Fidelidad del sitio web: es inevitable que el intento de eliminar el código activo malicioso y reconstruir HTML, CSS y arquitecturas de sitios poco comunes dé como resultado páginas dañadas que no se muestran correctamente o no se muestran en lo absoluto. Además, los sitios web que funcionan hoy puede que no lo hagan mañana, ya que los editores de sitios pueden hacer cambios diarios que pueden romper la funcionalidad de reconstrucción del DOM. La manipulación del DOM incluso tiene dificultades para admitir servicios comunes para la empresa como Google G Suite o Microsoft Office 365. El resultado es una sucesión infinita de problemas que requieren recursos informáticos significativos que tratan de abordar sin éxito las mismas cuestiones.

Altos costos: algunos servicios de manipulación del DOM se alojan en una infraestructura de nube pública de terceros, lo que implica costos adicionales que normalmente se transfieren a los clientes. De cualquier manera, la organización permanecerá expuesta, ya sea a través de empleados no protegidos o a través de sitios "fiables" que se han visto comprometidos

Vulnerabilidades de seguridad: al igual que con la "inserción de píxeles", la experiencia poco fiable del usuario final de la manipulación del DOM significa a menudo que las organizaciones solo la utilizan de forma puntual. Además, aunque la manipulación del DOM es una forma de aislamiento del navegador, sigue enviando código de terceros no fiable a los dispositivos de punto de conexión. Si el servicio no identifica el código malicioso, lo cual es un riesgo permanente dado el panorama de amenazas en constante evolución, los dispositivos de punto de conexión podrían sucumbir.



Aislamiento de la actividad de navegación en una máquina virtual en el dispositivo

En este enfoque, el software instalado en un dispositivo de punto de conexión crea una máquina virtual que está aislada del resto del sistema operativo del dispositivo. Toda la actividad de navegación tiene lugar en esta máquina virtual, por lo que cualquier malware descargado no puede infectar al resto del dispositivo. Además, al igual que otros enfoques, el software puede marcar ciertas páginas como riesgos de phishing.

Lamentablemente, los problemas inherentes a este enfoque son:

- **Alta capacidad de CPU y RAM:** la ejecución de una máquina virtual independiente puede ralentizar muchos equipos personales, lo que empeora las experiencias de navegación de los usuarios finales.
- **Dificultades en la gestión de puntos de conexión:** el aislamiento del navegador mediante software local requiere que los equipos informáticos instalen y actualicen dicho software en cada dispositivo de punto de conexión, una tarea difícil para las grandes organizaciones. Esta complejidad logística se agrava aún más cuando las organizaciones tienen un gran número de trabajadores remotos, o si contratan los servicios de proveedores externos que no utilizan los dispositivos proporcionados por la empresa.
- **Problemas de compatibilidad móvil:** el aislamiento del navegador basado en una máquina virtual en el dispositivo requiere implementaciones específicas del sistema operativo. Los dispositivos móviles a menudo no son compatibles.
- **Errores de aislamiento:** los servicios de aislamiento de navegadores locales sufren de forma periódica vulnerabilidades que permiten que el código malicioso acceda al sistema operativo principal. En estas circunstancias, los equipos informáticos o los usuarios finales deben instalar manualmente parches y actualizaciones. Sin embargo, si el parche no se instala correctamente, el dispositivo final puede quedar expuesto.
- **Experiencia del usuario final poco satisfactoria:** las implantaciones basadas en máquinas virtuales suelen requerir que los usuarios finales utilicen navegadores, ventanas o escritorios "virtualizados" independientes. Esta práctica requiere formación y supone una carga para los equipos informáticos.

Estos desafíos inmediatos crean otros nuevos

Las consecuencias inmediatas, como los altos costes, las malas experiencias de los usuarios finales y las dificultades de administración de los puntos de conexión, no son los únicos desafíos que plantean los enfoques comunes del aislamiento del navegador.

Otros retos son las consecuencias a largo plazo del riesgo al que se exponen los dispositivos. Cuando los usuarios finales inician sesión en aplicaciones sensibles a través de un dispositivo vulnerable, el malware puede acceder a los datos de esa aplicación sin que el usuario sea consciente.

Además, todos estos enfoques del aislamiento del navegador tienen dificultades para evitar ciertos tipos de pérdida de datos. Es posible que los empleados internos puedan cargar y enviar información confidencial por correo electrónico o introducirla en formularios en línea.

Cómo mejorar el enfoque del aislamiento remoto del navegador

Las organizaciones siguen queriendo adoptar la navegación remota a pesar de los problemas mencionados en la sección anterior.

Por suerte, algunas tecnologías pueden ayudar:

Problema	Solución
 Latencia	**Uso de una gran red perimetral:** en lugar de alojar el aislamiento del navegador en un número limitado de centros de datos de la nube pública, hazlo en una red perimetral global que esté cerca de los usuarios finales en cualquier lugar. Además, utiliza un software de aislamiento del navegador que se aloje en los mismos centros de datos que las puertas de enlace web seguras y otras herramientas de seguridad.
 Altos requisitos de ancho de banda	**Sin inserción de píxeles:** la transmisión de imágenes de la actividad del navegador remoto no es práctica para implementar en empresas más grandes, tanto desde el punto de vista del coste como de la experiencia del usuario.
 Fidelidad del sitio web	**Uso de tecnología de navegación nativa:** los navegadores remotos que utilizan tecnología ya integrada en las aplicaciones comunes de navegación de dispositivos finales son más fiables para reconstruir todo tipo de sitios con precisión.
 Altos costes de computación	**Computación en la nube de próxima generación:** evita el aislamiento remoto del navegador alojado en la nube pública y utiliza técnicas eficientes de computación sin servidor que mejoren la virtualización y la contenerización, eliminando al mismo tiempo la orquestación y la gestión de los recursos del servidor subyacente con el fin de utilizar esos recursos de manera más eficaz.
 Fallos de seguridad	**Uso de tecnología de navegación nativa:** en lugar de intentar decidir qué código enviar o bloquear, la tecnología de navegación nativa puede evitar enviar el código por completo. En su lugar, puede enviar solo el último paso en el proceso de renderizado en pantalla que dibuja la página.
 Dificultades específicas del punto de conexión	**Sin aislamiento del navegador local:** el aislamiento de la actividad de navegación en los dispositivos de punto de conexión es demasiado lento y difícil de administrar, lo que hace que el enfoque sea completamente obsoleto.

Para ver cómo funcionan estas tecnologías en la práctica, considera el ejemplo de aislamiento del navegador de Cloudflare, que está integrado de forma nativa con nuestra plataforma Zero Trust.

Cómo consigue Cloudflare que la navegación remota sea rentable y menos problemática para el usuario final

Cloudflare evita a gran escala las dificultades específicas del punto de conexión con solo operar en una red perimetral global en lugar de en dispositivos de punto de conexión. Más en concreto, la tecnología de Cloudflare elimina también otros problemas:

Problema	Solución	Implementación de Cloudflare
Latencia	Uso de una red perimetral potente	El aislamiento remoto del navegador tiene lugar en todos los centros de datos de la red perimetral de Cloudflare, que abarca más de 200 ciudades en 100 países y se encuentra a 100 milisegundos del 95 % de la población mundial conectada a Internet. Esta misma infraestructura ofrece servicios globales de DNS y CDN de latencia ultrabaja. Además, nuestra navegación remota interactúa fácilmente con nuestro servidor proxy de reenvío para aplicar todos los demás filtros (como bloquear parte de una página) e inspecciones sin necesidad de múltiples pasos y saltos entre soluciones de punto dispares.
Altos requisitos de ancho de banda	Tecnología de navegación nativa	La tecnología Network Vector Rendering de Cloudflare (más información a continuación) transmite los comandos de dibujo en lugar de imágenes de píxeles o código "filtrado". Este método requiere solo una parte del ancho de banda que consume la navegación normal o la manipulación del DOM, por no hablar de la "inserción de píxeles".
Fidelidad del sitio web	Tecnología de navegación nativa	El navegador remoto de Cloudflare se basa en el motor Chromium de código abierto, sobre el que se desarrolla Google Chrome y otros 21 navegadores comunes. La importante inversión en marcha en el motor Chromium garantiza los más altos niveles de compatibilidad de los sitios web. Además, como la tecnología Network Vector Rendering de Cloudflare transmite comandos de dibujo en lugar de código "limpio", garantiza que incluso las páginas web más complejas no se dañen.
Altos costes de computación	Computación en la nube de próxima generación	Como el aislamiento del navegador de Cloudflare funciona en nuestra propia red, no tenemos que repercutir los costes de la nube pública a los clientes. Además, podemos orquestar y administrar los recursos del servidor de manera muy eficiente, por lo que evitamos los arranques en frío de segundos de duración que frecuentemente afectan a las aplicaciones alojadas en la nube pública.
Fallos de seguridad	Tecnología de navegación nativa	Al transmitir comandos ligeros de dibujo vectorial, en lugar de cualquier código de sitio web original, Cloudflare elimina el riesgo de que se ejecute un código que no es de confianza en el dispositivo de punto de conexión. El malware no detectado solo compromete el navegador remoto sin afectar al punto de conexión. Y dado que Cloudflare ofrece experiencias sólidas a los usuarios finales, las empresas pueden aplicar la navegación remota a casos de uso menos arriesgados que, de otro modo, podrían quedar desprotegidos.
	Control granular del comportamiento del usuario final	Las herramientas de prevención de pérdida de datos suelen proteger los datos mientras están en tránsito por la red, ya sea permitiendo o bloqueando la transmisión. Cloudflare Browser Isolation otorga a los administradores un control granular sobre: • Permisos para copiar/pegar/imprimir • Acciones para cargar/descargar • Actividad del teclado en general • Permisos de entrada de formularios • Dónde se almacenan los archivos descargados * *Próximamente

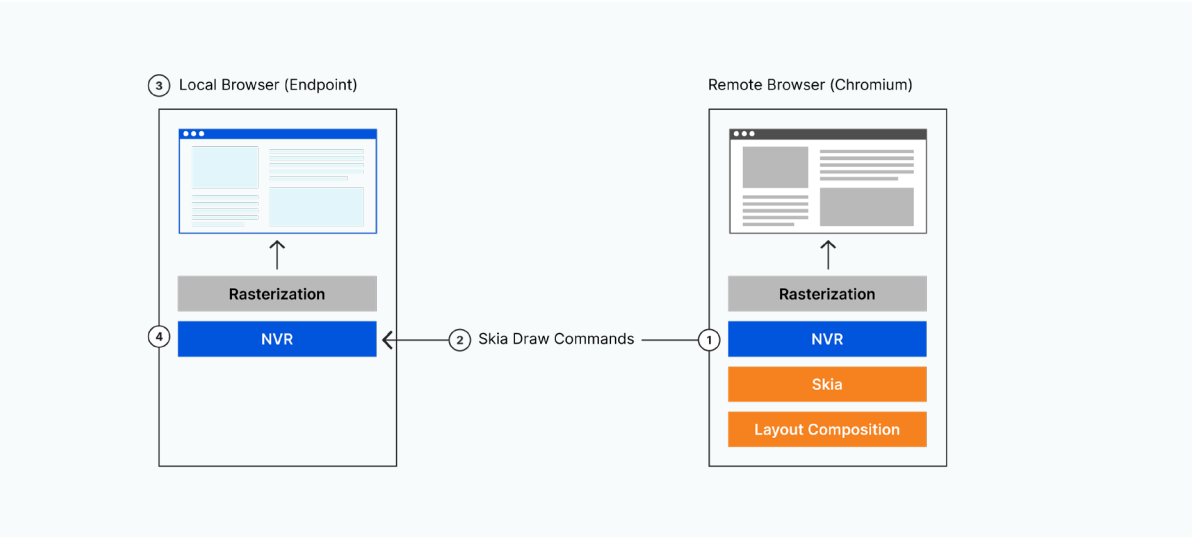
Sigue leyendo para descubrir más información sobre la técnica Network Vector Rendering descrita anteriormente:

Network Vector Rendering ofrece mejores experiencias al usuario final y reduce las vulnerabilidades de seguridad

Como se ha mencionado anteriormente, el navegador remoto de Cloudflare está basado en Chromium. Una función arquitectónica clave del navegador Chromium es el uso de Skia, un motor gráfico multiplataforma muy utilizado para Android, Google Chrome, Chrome OS, Mozilla Firefox y muchos otros navegadores. Todos los navegadores compatibles con HTML5 pueden renderizar Skia. Todo lo visible en una ventana del navegador Chromium se renderiza a través de la capa de renderizado de Skia. Esto incluye la interfaz de usuario de la ventana de la aplicación, como los menús, pero lo que es más importante, todo el contenido de la ventana de la página web se representa a través de Skia. Cloudflare puede incluso aislar los archivos descargados y moverlos a varias ubicaciones según las necesidades del usuario final.

La tecnología Network Vector Rendering (NVR) de Cloudflare intercepta los comandos de dibujo de Skia del navegador Chromium remoto, los convierte en token y los comprime, luego los cifra y los transmite por cable a cualquier navegador web compatible con HTML5 que se ejecute localmente en el escritorio del punto de conexión o dispositivo móvil. Los comandos de la API de Skia capturados por NVR se pre-rasterizan, lo que significa que son muy compactos. Y como Skia está tan extendido, la navegación remota de Cloudflare funciona en cualquier navegador web moderno.

La tecnología Network Vector Rendering también es más segura. Como hemos mencionado anteriormente, dado que Cloudflare entrega comandos de dibujo en lugar de código real del sitio web a los dispositivos de punto de conexión, el transporte de datos subyacente no es un vector de ataque.



Más información - cómo empezar

Desde que Cloudflare empezó su andadura, nuestra misión ha sido mejorar Internet y democratizar las tecnologías que antes solo eran accesibles para las grandes empresas con redes sofisticadas, equipos de TI dedicados y enormes presupuestos. Mejorar el aislamiento remoto del navegador es una parte importante de esa misión.

Al garantizar un aislamiento del navegador más rentable y ofrecer experiencias excepcionales a los usuarios finales, esperamos que más organizaciones puedan experimentar el verdadero valor de la tecnología. Al igual que en un pasado no demasiado lejano, cuando el cifrado HTTPS se reservaba para páginas de inicio de sesión "sensibles" y pagos de comercio electrónico, creemos que confiar en el código arbitrario del sitio web parecerá tan arcaico como crear el nuevo paradigma de la navegación Zero Trust.

Para saber más sobre Cloudflare Browser Isolation y cómo puede ayudarte a conseguir una navegación Zero Trust, visita https://www.cloudflare.com/products/zero-trust/browser-isolation/

© 2022 Cloudflare Inc. Todos los derechos reservados. El logotipo de Cloudflare es una marca comercial de Cloudflare. Todos los demás nombres de empresas y productos pueden ser marcas comerciales de las respectivas empresas a las que están asociados.