Aislamiento remoto del navegador (RBI)

Aísla a los usuarios de las amenazas en línea y protege los datos en las aplicaciones con controles de navegador eficaces.

Protege la primera línea del trabajo moderno

Hoy en día, el navegador es fundamental para las actividades comerciales diarias, lo que plantea riesgos como objetivo para los atacantes y como entorno para filtrar datos. Sin embargo, los controles a través del RBI tradicional o la infraestructura de escritorio virtual (VDI) históricamente han generado experiencias frustrantes para los usuarios, implementaciones complejas y costos elevados.

El aislamiento del navegador de Cloudflare simplifica la protección contra amenazas y de datos, al mismo tiempo que preserva una experiencia de navegación nativa. Al ejecutar todo el código web en nuestra red global en la nube (en lugar de hacerlo localmente en los dispositivos), las organizaciones pueden eliminar los riesgos comunes:

- **Aísla la navegación web** para proteger a los usuarios de las ciberamenazas, incluidas las amenazas zero-day
- **Aísla las aplicaciones** de los empleados, terceros y dispositivos no gestionados para bloquear los datos en uso
- **Aísla las herramientas de IA** para restringir el intercambio excesivo de información privada

Aislamiento dentro de la arquitectura SSE de Cloudflare

El aislamiento del navegador de Cloudflare está diseñado desde cero en nuestra red para funcionar de forma nativa con nuestros otros servicios modulares de seguridad en el perímetro (SSE).

Los controles de aislamiento funcionan junto con ZTNA, SWG, DLP, seguridad del correo electrónico y más para reducir el riesgo en entornos web, SaaS, correo electrónico y aplicaciones privadas.

¿Por qué Cloudflare?

Fácil de configurar y escalar

Para los dispositivos gestionados, implementa con un dispositivo del cliente. Para contratistas y dispositivos no gestionados, simplifica el aislamiento de destinos específicos a través de enlaces.

Compatible en cualquier página web con cualquier navegador.

UX rápida y uniforme a nivel global

Nuestro RBI está diseñado para ejecutarse en más de 300 ubicaciones en nuestra red global, de modo que las sesiones aisladas se brinden cerca de los usuarios finales, dondequiera que se encuentren.

Garantiza la seguridad y la productividad de los usuarios con la navegación receptiva.

Diseñado para Zero Trust

Aplica un enfoque de "nunca confiar" en la navegación en Internet, para que no se confíe en ningún contenido web por defecto.

Unifica la visibilidad y los controles de los servicios SSE, incluido el RBI, en una sola red y plano de control con Cloudflare.

Caso de uso: aislar la navegación web para defenderse de las amenazas

Neutraliza el malware, el ransomware, las amenazas zero-day y mucho más ejecutando todo el contenido web en la red de Cloudflare, lejos de los dispositivos de los usuarios.

Mitiga las amenazas de phishing evitando que los usuarios ingresen en sitios web peligrosos. Minimiza los riesgos de los enlaces desconocidos en el correo electrónico, los SMS, la mensajería instantánea, LinkedIn, las redes sociales y las aplicaciones de colaboración en la nube .

Aísla toda la navegación web

LUANA SAVINGS BANK

Servicios financieros
Leer el caso práctico

- **0 dispositivos infectados por malware** de la navegación en Internet desde la primera adopción de RBI.
- **12 horas mensuales ahorradas** para dos empleados al eliminar el tiempo de investigación de infecciones de malware

Comenzar

Pasos prioritarios

Implementación del dispositivo del cliente a través de una administración gestionada o una autoinscripción

Configuración de filtros DNS e inspecciones HTTP como capas iniciales de protección contra amenazas

Aislamiento de la navegación para dominios riesgosos o usuarios prioritarios

Ampliar controles

Implementación de la seguridad del correo electrónico en la nube para proteger las bandejas de entrada del phishing y aislar los enlaces sospechosos.

Caso de uso: aislar el acceso a las aplicaciones para proteger los datos, con/sin un dispositivo del cliente

Controla cómo los usuarios interactúan con los datos (p. ej. restringir copiar/pegar, cargas/descargas, entradas de teclado, impresión) aislando el acceso a aplicaciones específicas, incluidas las herramientas de IA.

La implementación sin cliente en sitios web y aplicaciones específicos ayuda a reducir los riesgos de exposición de datos que plantean proveedores, terceros y dispositivos no gestionados.

APPLIED

Tecnología de seguros
Leer el caso práctico

Aísla las herramientas de IA disponibles públicamente para evitar que los usuarios copien y peguen información confidencial en los LLM.

OpenAI Bard

Comenzar

Pasos prioritarios

Aislamiento de los destinos a través de una URL prefijada o aísla las aplicaciones autoalojadas por dominio, sin necesidad de un dispositivo del cliente.

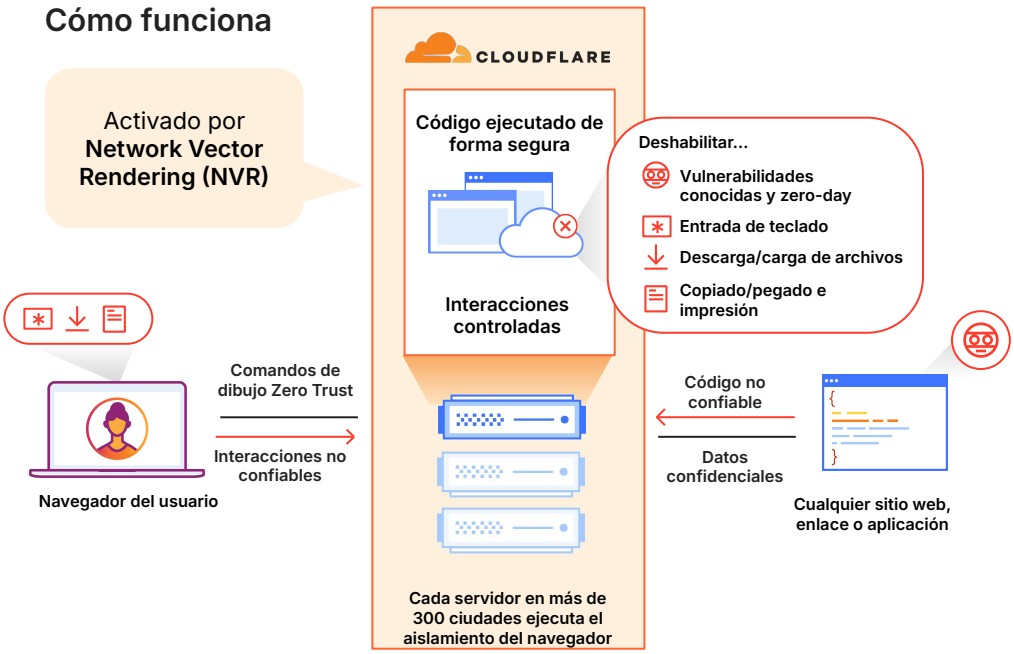
Implementación del dispositivo del cliente (si es necesario) para obtener una visibilidad más detallada y controles HTTP.

Establecimiento de controles de datos en uso: bloquea copiar/pegar, cargas/descargas, entradas de teclado o imprimir.

Ampliar controles

Bloqueo del movimiento de datos confidenciales con análisis y políticas de prevención de pérdida de datos (DLP).

Cómo funciona



Experiencia del usuario ultrarrápida con NVR

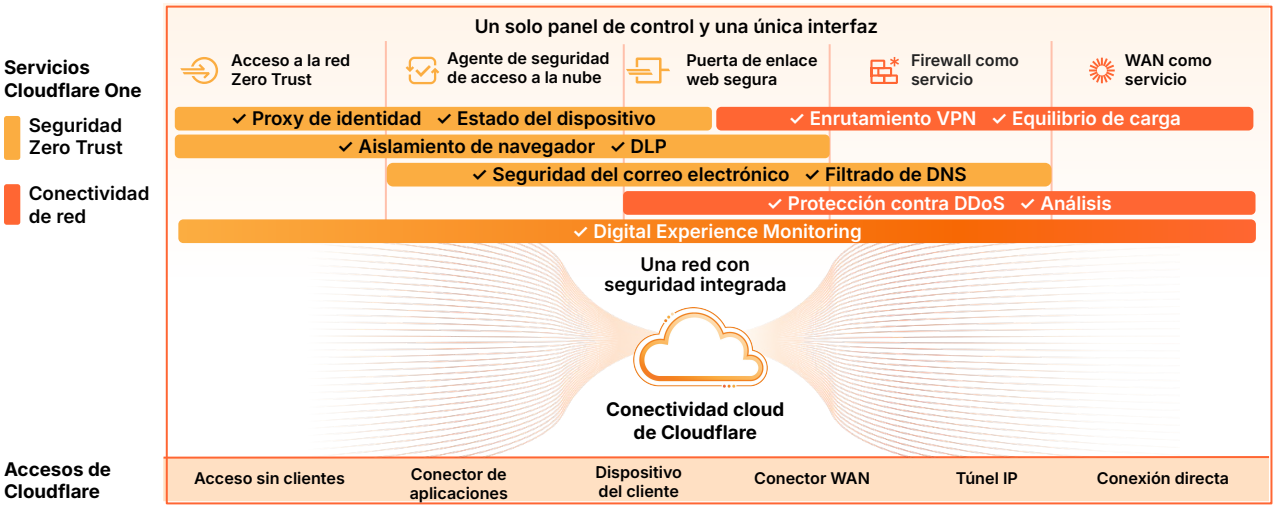
- Transmite comandos de dibujo seguros al dispositivo.
- Elimina la latencia de los métodos RBI tradicionales, como la inserción de píxeles o la reconstrucción de DOM.

Capacidades de muestra

Políticas	
Aislamiento por identidad, amenaza de seguridad o contenido	Aísla los sitios web en función de la identidad, las amenazas a la seguridad o el contenido. Cobertura integral de los riesgos de seguridad (p. ej., ransomware, phishing, dominios DGA), categorías de contenido (p. ej., entretenimiento) y aplicaciones (p. ej., inteligencia artificial, redes sociales).
Controles del navegador para datos en uso	Define políticas para restringir las entradas del teclado, la impresión y las cargas/descargas. Bloquea completamente el copiado y/o pegado — permite solo copiar y/o pegar dentro de un navegador aislado para evitar el movimiento de datos a los portapapeles locales. Exporta registros de seguimiento de estas acciones de los usuarios.
Funcionalidad completa de SWG	Controla el tráfico en función del origen, el destino, los dominios, los métodos HTTP, las URL y otros parámetros. La inspección HTTP1/2/3 permite el análisis AV y DLP, el estado del dispositivo, los inquilinos y mucho más. Inspección ilimitada de TLS 1.3 habilitada de forma predeterminada. Las claves TLS se almacenan con criptografía segura poscuántica.
Políticas de DLP para datos en tránsito	Analiza el tráfico HTTP en busca de datos confidenciales (p. ej., financieros, de salud, código fuente) y bloquéalo con políticas de prevención de pérdida de datos (DLP). Aplica en navegadores aislados con o sin un dispositivo del cliente.
Accesos	
Accesos basados en la identidad	Aplica políticas HTTP basadas en la identidad al tráfico redireccionado mediante proxy a través de nuestro dispositivo del cliente o a aplicaciones protegidas por nuestro servicio de acceso a la red Zero Trust (ZTNA).
Sin identidad	Aplica políticas HTTP sin identidad al tráfico reenviado a un punto final de proxy con archivos de configuración automática de proxy (PAC) o a través de un túnel GRE/IPsec.
Aislamiento web sin cliente	Representa páginas web en un navegador remoto cuando los usuarios van a la URL prefijada: https://<your-team-name>.cloudflareaccess.com/browser/<URL>.
Servicios extensibles	
Aislamiento de enlaces por correo electrónico	En combinación con Cloudflare Email Security, reescribe los enlaces sospechosos/desconocidos dentro de los correos electrónicos para abrirlos en un navegador aislado, protegiendo a los usuarios de las amenazas de phishing y malware.
Extensión del navegador	El aislamiento del navegador de Cloudflare admite la ejecución de extensiones web nativas de Chromium. Amplía las herramientas que requieren acceso al DOM (como los administradores de contraseñas y los bloqueadores de anuncios) a páginas aisladas. La extensión sincroniza las cookies entre el navegador local y el remoto, para que los usuarios puedan acceder sin problemas a aplicaciones aisladas y no aisladas sin necesidad de volver a autenticarse.

Moderniza la seguridad con la plataforma SSE/ SASE de Cloudflare

El aislamiento del navegador de Cloudflare es un servicio modular dentro de Cloudflare One, nuestra plataforma SSE/SASE. Las organizaciones suelen implementar RBI junto con ZTNA, SWG y otras capacidades para aumentar la seguridad web y del correo electrónico o para aplicar controles de datos detallados en entornos web, SaaS y de aplicaciones privadas.



Una plataforma unificada

- **Acceso seguro** mediante la verificación y la segmentación de cualquier usuario a cualquier recurso
- **Protección contra amenazas** que abarca todos los canales con información sobre amenazas y aprendizaje automático e IA basada en la red
- **Protección de datos** con mayor visibilidad y control de los datos en tránsito, en reposo y en uso

Una red programable

- **Más eficaz**, ya que simplifica la conectividad y la gestión de políticas.
- **Mayor productividad** al garantizar una experiencia del usuario rápida, fiable y coherente en todas partes.
- **Más ágil**, gracias a su capacidad para innovar rápidamente y satisfacer tus nuevos requisitos de seguridad.

¿Quieres experimentar la navegación aislada con Cloudflare?

Pruébalo ahora, no requiere instalación

¿O quieres modernizar la seguridad de tu navegador?

Solicitar seminario