CLOUDFLARE

PRODUCT OVERVIEW

Remote Browser Isolation (RBI)

Insulate users from threats online and protect data in applications with seamless browser controls.

Secure the frontline of modern work

Today, the browser is core to everyday business, posing risks as a target for attackers and as an environment to leak data. However, controls through traditional RBI or virtual desktop infrastructure (VDI) have historically led to frustrating user experiences, complex deployments, and high costs.

Cloudflare Browser Isolation simplifies threat and data protection while preserving a native browsing experience. By running all web code on our global cloud network (instead of locally on devices), organizations can eliminate common risks:

- **Isolate web browsing** to safeguard users from cyber threats, including zero-days
- **Isolate apps** for employees, third-parties, and unmanaged devices to lock down data-in-use
- **Isolate AI tools** to restrict oversharing of proprietary information

Isolation within Cloudflare's SSE architecture

Cloudflare Browser Isolation is built from the ground up on our network to work natively with our other composable Security Services Edge (SSE) services.

Isolation controls work alongside ZTNA, SWG, DLP, email security, and more to reduce risk across web, SaaS, email, and private app environments.

Why Cloudflare?

Simple to set up and scale

For managed devices, deploy with a device client. For contractors and unmanaged devices, simplify isolate specific destinations via links.

Compatible on any webpage with any browser.

Fast, consistent UX globally

Our RBI is designed to run across 300+ locations on our global network, so that isolated sessions are delivered close to end users wherever they are.

Keep users safe and productive with responsive browsing.

Architected for Zero Trust

Apply a "never trust" approach to Internet browsing, so that no web content is trusted by default.

Unify visibility and controls across SSE services, including RBI, on one network and control plane with Cloudflare.

Use case: Isolate web browsing to defend against threats

Neutralize malware, ransomware, zero-day threats, and more by executing all web content on Cloudflare's network — far away from user devices.

Mitigate phishing threats by preventing user input on risky websites. Minimize risks from unknown links within email, SMS, IM, LinkedIn, social media, and cloud collaboration apps.

Isolate all web browsing

LUANA SAVINGS BANK

Financial services
Read case study

- **0 devices infected by malware** from Internet browsing since first adopting RBI
- **12 hours saved monthly** for two employees by eliminating time investigating malware infections

Getting started

Priority steps

Deploy device client via managed or self-serve enrollment

Configure DNS filters and HTTP inspections as initial layers of threat defense

Isolate browsing for risky domains or priority users

Expand controls

Deploy cloud email security to protect inboxes from phishing and isolate suspicious links.

Use case: Isolate app access to protect data — with/without a device client

Control how users interact with data (e.g. restrict copy/paste, uploads/downloads, keyboard inputs, printing) by isolating access to specific apps, including AI tools.

Clientless deployment to specific websites and apps helps reduce data exposure risks posed by contractors, third-parties, and unmanaged devices.

APPLIED

Insurance technology
Read case study

Isolate publicly available AI tools to prevent users from copying and pasting sensitive info into LLMs.

OpenAI Bard

Getting started

Priority steps

Isolate destinations via a prefixed URL or isolate self-hosted apps by domain — no device client required

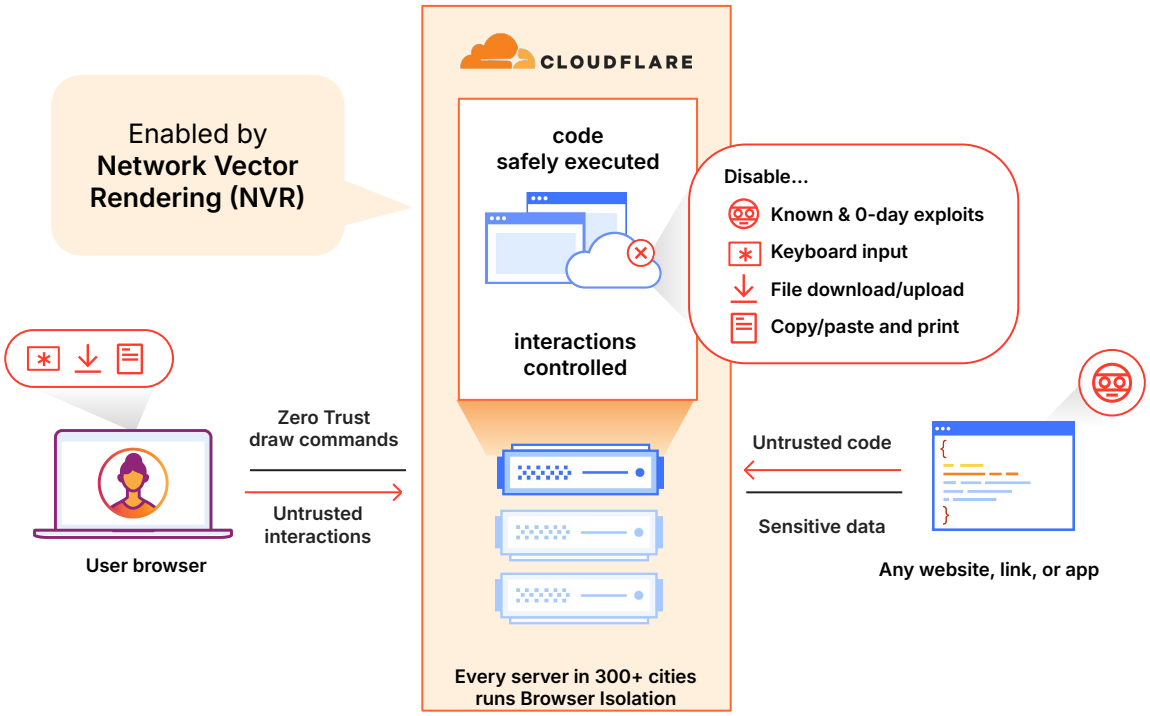
Deploy device client (if needed) for more granular visibility & HTTP controls

Set data-in-use controls: block copy / paste, uploads / downloads, keyboard inputs, or printing

Expand controls

Block movement of sensitive data with data loss prevention (DLP) scanning and policies.

How it works



Lightning-fast user experience with NVR

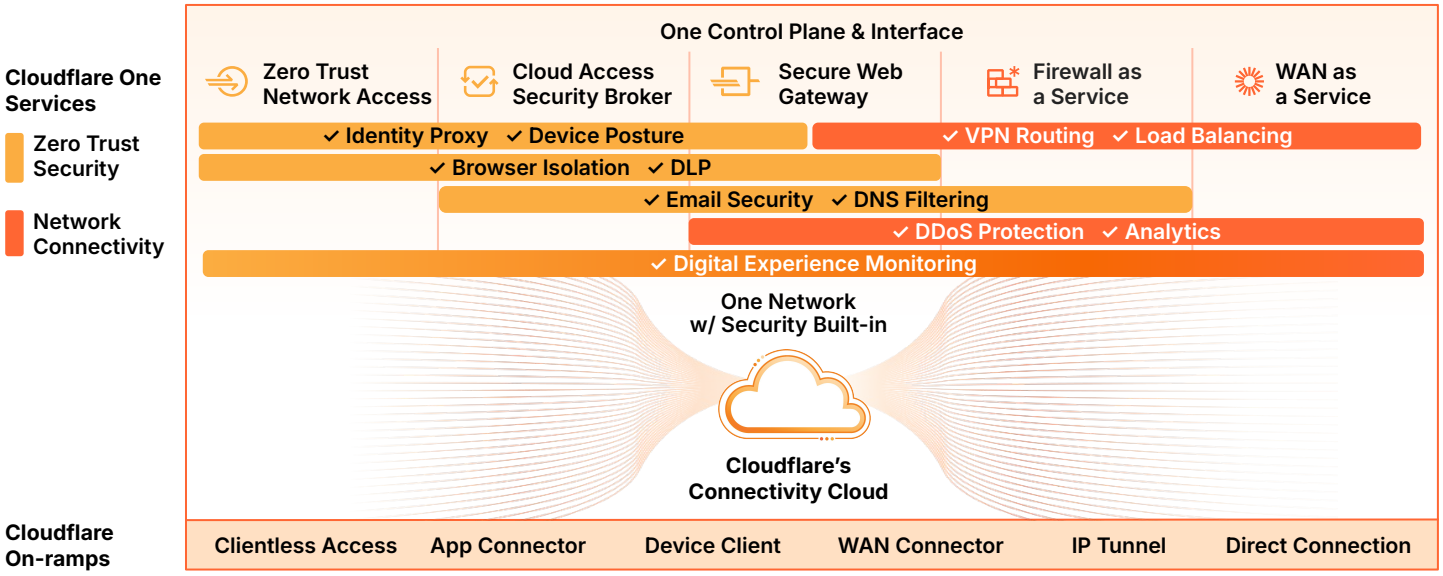
- Stream safe draw commands to the device.
- Eliminate latency of traditional RBI methods like pixel-pushing or DOM reconstruction.

Sample capabilities

Policies	
Isolate by identity, security threat or content	Isolate websites based on identity, security threats, or content. Comprehensive coverage of security risks (e.g. ransomware, phishing, DGA domains), content categories (e.g. entertainment), and applications (e.g. artificial intelligence, social networking).
Browser controls for data-in-use	Define policies to restrict keyboard inputs, printing, and uploads / downloads. Block copy and/or paste entirely — only allow copy and/or paste within an isolated browser to prevent movement of data to local clipboards. Export logs tracking these user actions.
Full SWG functionality	Control traffic based on source, destination, domains, HTTP methods, URLs, and other criteria. HTTP1/2/3 inspection enables AV & DLP scans, device posture, tenants, and more. Unlimited TLS 1.3 inspection enabled by default. TLS keys are stored with post-quantum safe cryptography.
DLP policies for data-in-transit	Scan HTTP traffic for sensitive data (e.g. financial, health, source code) and block with data loss prevention (DLP) policies. Apply in isolated browsers with or without a device client.
On-ramps	
Identity-based on-ramps	Apply identity-based HTTP policies to traffic proxied through our device client or to applications protected by our Zero Trust Network Access (ZTNA) service.
Non-identity	Apply non-identity HTTP policies to traffic forwarded to a proxy endpoint with proxy auto-configuration (PAC) files or through a GRE / IPsec tunnel.
Clientless web isolation	Render web pages in a remote browser when users go to prefixed URL: https://<your-team-name>.cloudflareaccess.com/browser/<URL>.
Extendable services	
Email link isolation	In combination with Cloudflare Email Security, rewrite suspicious / unknown links within emails to open in an isolated browser, insulating users from phishing and malware threats..
Browser extension	Cloudflare Browser Isolation supports running native Chromium Web Extensions. Extend tools that require DOM access (such as password managers and ad blockers) to isolated pages. The extension syncs cookies between the local and remote browser, so users can seamlessly access isolated and non-isolated apps without needing to re-authenticate.

Modernize security with Cloudflare's SSE/SASE platform

Cloudflare Browser Isolation is a composable service within Cloudflare One, our SSE/SASE platform. Organizations typically deploy RBI alongside ZTNA, SWG, and other capabilities to augment web and email security or to enforce granular data controls across web, SaaS, and private app environments.



One unified platform

- **Secure access** by verifying and segmenting any user to any resource
- **Threat defense** by covering all channels with network-powered AI/ML and threat intel
- **Data protection** by increasing visibility and control of data in transit, at rest, and in use

One programmable network

- **More effective** by simplifying connectivity and policy management
- **More productive** by ensuring fast, reliable, and consistent UX everywhere
- **More agile** by innovating rapidly to meet your evolving security requirements

Want to experience isolated browsing with Cloudflare?

Try it now — no installation required

Or, ready to modernize your browser security?

Request a workshop