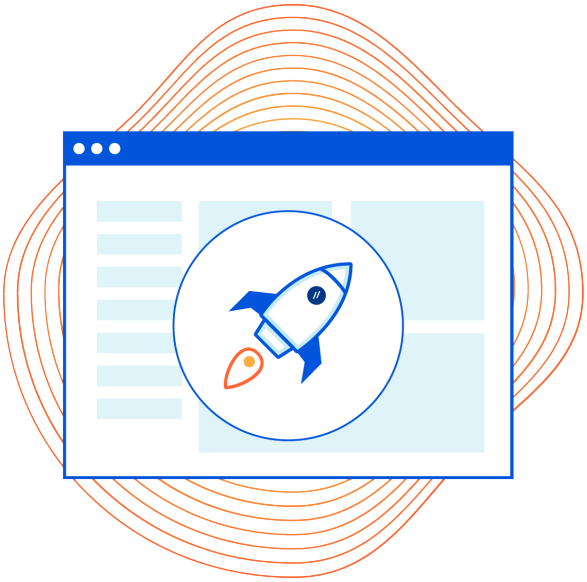
Zero Trust Browsing

New remote browser isolation service runs in the cloud away from your networks and endpoints, drastically reducing the attack surface and stopping unknown malware.

No IT team can keep every browser patched against known vulnerabilities, and no secure web gateway can block every threat. Executing browser code in the cloud, instead of on the endpoint, helps solve these problems, but existing technologies have unreliable rendering and poor performance. Cloudflare's new remote browser isolation service stops malware before it infects endpoints, and the experience feels like a local browser.

Not your average remote browser



Compatibility

Works natively in existing browsers.

Performance

Delivers a low latency stream of the webpage.

Browser Isolation now comes natively integrated in the Cloudflare for Teams policy builder, allowing administrators to allow, block, or isolate any security or content category and application group. Filtering, inspection and isolation rules are applied in one lightning-fast single pass inspection.

Attacks will strike. Mitigate the impact.

Reduce attack surface

Zero Trust browsing stops malicious code on uncategorized, risky, or even low-risk sites from infecting users' devices.

Simplify deployment

With Cloudflare for Teams, set Zero Trust browsing policies in the same place you manage application access.

Coming soon: protect data

Stop data loss and phishing by controlling user actions (keyboard input, copy, print, up/download) within applications or risky sites.

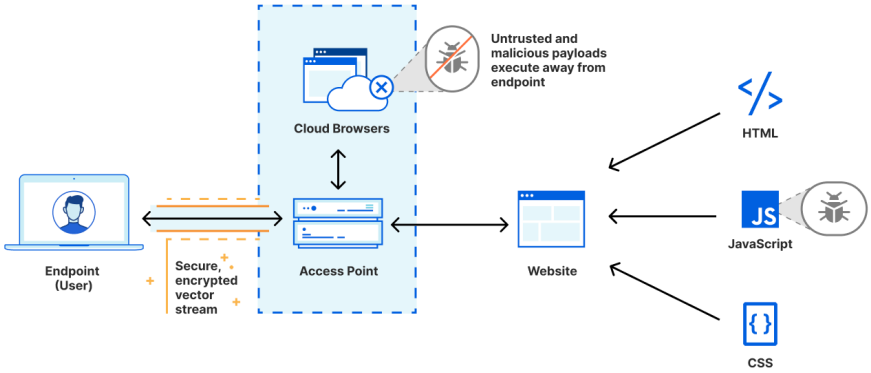
Local vs Remote Browsing: what's different?

Local

Untrusted web page code and phishing sites execute locally on the endpoint device. Users can freely input sensitive data into phishing websites and their devices and data are directly exposed to unpatched or zero-day threats.

Remote

Unfiltered code or sites can be executed in a continuously-patched remote browser. User interaction is controlled to prevent malware and phishing attacks and zero-day attacks are cordoned from the end-user's device.



The Cloudflare Difference

Network Vector Rendering

Unlike bandwidth-heavy pixel pushing or fragile content-disarm and reconstruction techniques, NVR streams safe draw commands to the device without transmitting any malicious web page code or impacting the end user experience.

Cloudflare Global Network

Other providers host remote browsers in public cloud providers. Cloudflare positions browsers closer to your users for an experience that feels no different than local browsing, anywhere.

Key Features

- Protect devices from malicious content
- Protect users from phishing sites
- Execute all browser code in the cloud
- Mitigate the impact of attacks
- Seamless, lightning-fast end user experience
- Recursive DNS Filters
- Layer 7 Proxy Filters
- Antivirus inspection
- CASB-lite
- Categorized application groups for Shadow IT visibility
- Identity-based country and device detail views
- Push logs to cloud storage or SIEMs
- Security categories (13) via machine learning and threat intelligence feeds
- Content categories (100+) for acceptable use
- Custom block, allow, or decryption bypass lists
- Granular HTTP and URL rules
- Fastest, intelligent IP routing (<100ms)
- Fastest, global edge network (200+ PoPs)
- Fastest, global policy updates (<5 seconds)
- 100% uptime SLA