Browser Isolation: Built-in Zero Trust for the Internet

Extending Zero Trust to the Internet

Large attack surface, limited controls

Today, the web browser is the most widely used corporate application — representing a large attack surface.

Yet historically, protecting users from browser-based threats has been imperfect. And applying controls to safeguard how users interact with sensitive has been even harder.

Perfecting Zero Trust

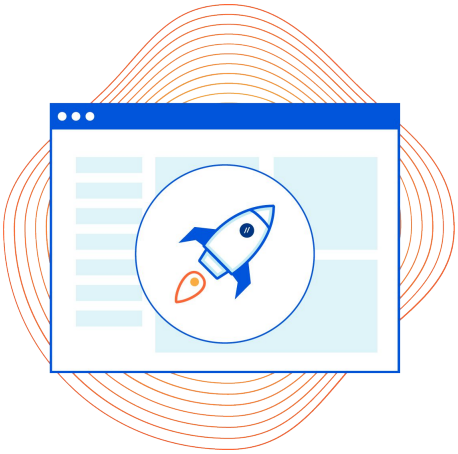
Applying Zero Trust to browsing means that no code or interactions should be trusted to run on devices by default.

Cloudflare Browser Isolation runs all code at our edge — insulating users from untrusted web content and protecting data in browser interactions from untrusted users and devices.

Not your average remote browser

- Compatibility works natively on any webpage, in any browser.
- Performance delivers a low latency stream of the webpage.

Cloudflare Browser Isolation secures data in-use from untrusted users and devices, and protects devices and users from ransomware and phishing — even zero-day attacks.



Built-in, not bolt-on security

Built on Cloudflare

Our browser isolation is built from the ground up with our other Zero Trust services on our network and designed to run across our 270+ locations.

Web browsing sessions are served as close to users as possible, ensuring a lightning-fast experience.

Natively integrated

Unlike other providers, Cloudflare has natively-integrated browser isolation with all our Zero Trust services.

Use a single management interface for:

- Secure web gateway (SWG)
- Zero trust network access (ZTNA)
- Cloud access security broker (CASB)
- Cloud email security (on roadmap)
- ...and more

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

Simplify deployment
Set Zero Trust browsing policies in the same place where you manage application access.

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

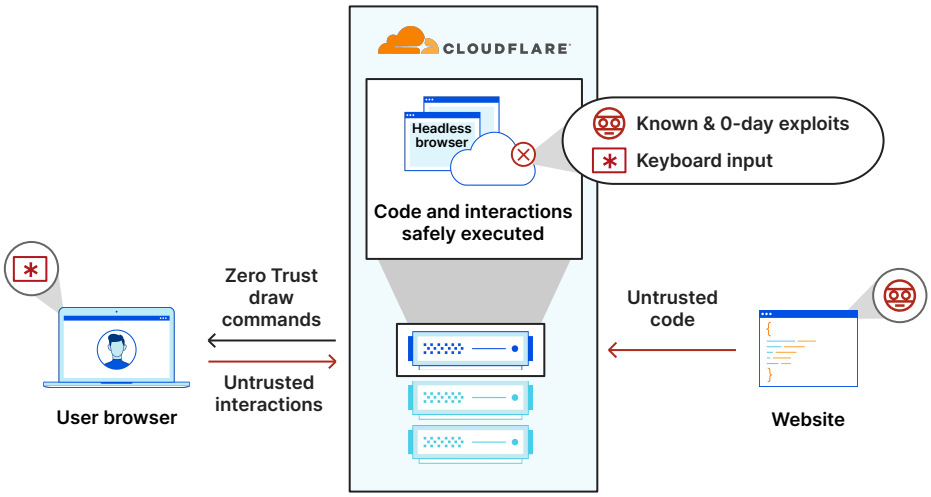
Threat protection

Minimize your attack surface without compromising user experience

Challenge:
No IT team can keep every browser patched against known vulnerabilities. Plus, the reality is that filters and inspections will never prevent or detect 100% of threats even with the best intel. Blocking every site is also not the answer: excessive restrictions could cause more damage in lost user productivity.

Solution:
Our Browser Isolation runs a headless version of the Chromium browser, which renders all browser code at our edge, instead of on your endpoints, to mitigate known and unknown threats like malware. The low-latency experience is invisible to end users and feels like a local browser.

How it works



Deployment *with* a device client
Send user traffic from devices to Cloudflare's global network for full L4-7 filtering and inspection.

Clientless deployment
Send users to an isolated hyperlink without exposing their public IP or device to potential malicious code on the site.

Key use cases

Ransomware

Isolation effectively protects against ransomware infection. But even for non-isolated sites, that defense is bolstered by native integrations with services like our SWG to block risky sites and domains and our ZTNA to reduce lateral movement of threats.

Phishing and email security

Isolation not only stops harmful code in a phishing link from executing locally, but also prevents keyboard inputs of sensitive personal info. Plus, coming soon, admins will be able to activate email filtering with a single click – powered by Area 1.

Zero-day attacks

When a patch is available for the zero-day vulnerability, Cloudflare automatically deploys the patch to all remote browsers on our network. This means admins can protect devices while avoiding interruptions do not need to interrupt users from their work to force updates.

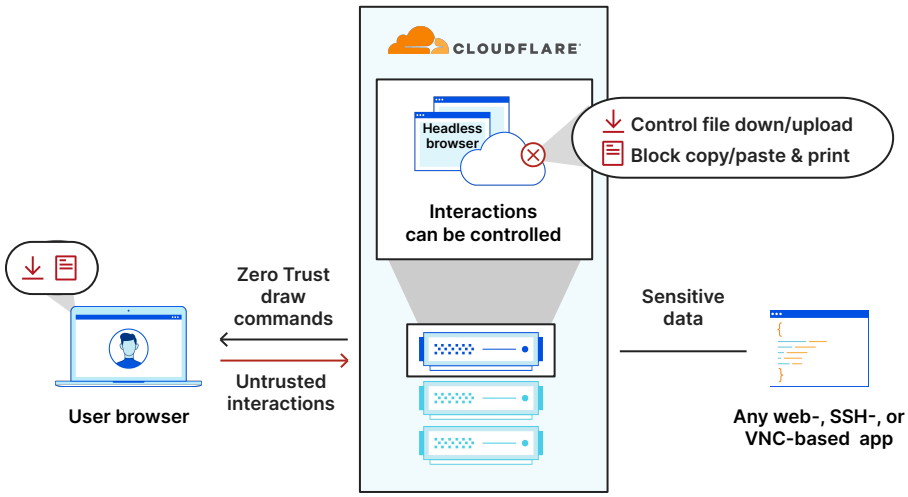
Data protection

Secure data in use within web browsers

Challenge:
The rise of SaaS software has made the web browser the primary way users access data. But traditionally, admins have had limited controls over how data once delivered to the browser. Users typically can copy, paste, or print sensitive data or PII into other websites, apps, or locations. These common actions increase the risk of a data breach.

Solution:
Running an isolated browser restores control to admins to protect sensitive data on any website or SaaS application. With just a few clicks, admins can build granular rules preventing risky user actions within the browser. This includes restricting download, upload, copy-paste, keyboard input, and printing functionalities.

How it works



Deployment *with* a device client
Gain full visibility and create device posture aware policies over how users on managed devices interact with data.

Clientless deployment
Isolate apps with sensitive data (like a CRM) that users on unmanaged devices are most likely to access regularly.

Key use cases

Secure contractor access

Isolate connections to specific hyperlinks — without installing any software on user devices.

Use this clientless model to protect data that contractors interact with on unmanaged devices — without added configuration overhead.

Control input on suspicious sites

Admins can protect teams by isolating these high-risk websites like 'Typosquatting' and 'Domains' often used for phishing. Cloudflare serves the site in read-only mode and disables file uploads, downloads and keyboard input.

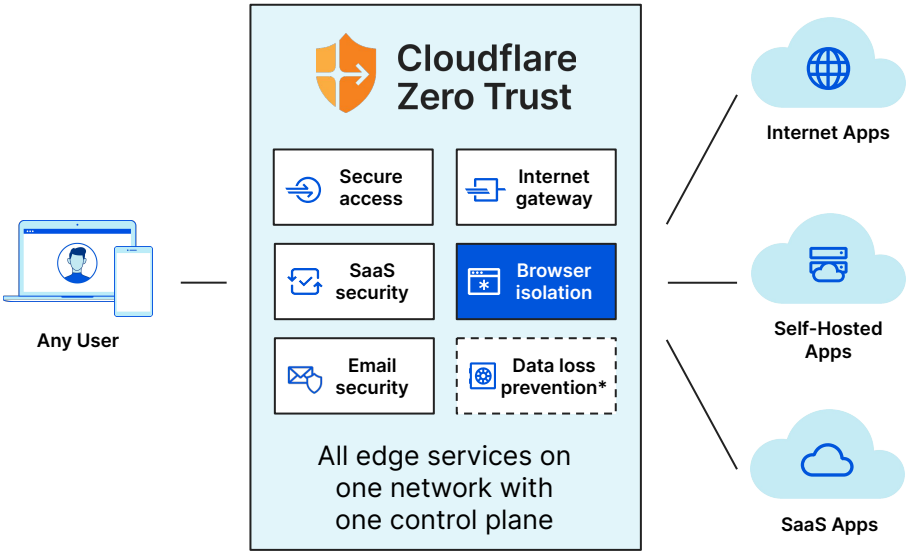
Integrate with third-party solutions

With our clientless deployment, admins can integrate Cloudflare with existing web or email gateways for a more gradual transition from legacy services. Send high-risk clicks to our remote browser and apply a custom block page or other protections.

The Cloudflare difference

Browser Isolation: Fundamental to Zero Trust

Isolation is a core Zero Trust principle. Extending visibility and controls into the browser is as easy as a few clicks with Cloudflare's Zero Trust platform.



*Join our DLP waitlist

Isolation made approachable
Historically, browser isolation existed as a standalone solution that only large enterprises could justify purchasing because of high cost and complexity.

With Cloudflare, native integrations with ZTNA, SWG, and other SSE services make it easy to begin your security modernization journey where it makes sense before extending Zero Trust further with browser isolation.

Local vs. remote browsing

Local browsing
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 browsing
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.

Cloudflare's approach

Network Vector Rendering (NVR)
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.

Our 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

- Execute all browser code in the cloud far from users
- No pixel pushing
- Lightning-fast network (<50ms away from 95% of Internet users globally)
- Compatibility with all modern browsers
- Deploy with or without a device client
- Stop data from leaving corporate apps and gain Shadow IT visibility
- Block threats with intelligence from our network firewall and Zero Trust rules
- 100% uptime SLA