

WHITEPAPER

# Redefining browser isolation security

How to solve the top four limitations  
of remote browsing



# Content

<b>04</b>	<b><u>Introduction: The amplification of web-based threats</u></b>
<b>05</b>	<b><u>The limitations of legacy browser isolation approaches</u></b>
06	Top four challenges with common RBI methods
<b>08</b>	<b><u>Modern RBI technology delivers more scalable and transparent protection</u></b>
08	How NVR reinvents the foundation of remote browsing
09	The benefits of using modern RBI technology
<b>11</b>	<b><u>Key use cases for modern RBI technology</u></b>
11	Stop multi-channel phishing attacks
12	Insulate users from malware
13	Isolate contractors and high-risk users
14	Minimize the risk of zero-day browser vulnerabilities
<b>15</b>	<b>Conclusion</b>

# Introduction: The amplification of web-based threats

As applications, users, and devices have ventured beyond the confines of the traditional corporate perimeter, security teams can no longer rely on location-centric methods to deliver consistent protections and safeguard data. During the ongoing accelerated shift to hybrid work, legacy security approaches have faltered — leaving organizations with inadequate visibility, conflicting configurations, and heightened risk.

Even with some employees returning to the office after years of pandemic-induced remote work, it's evident that the 'work-from-anywhere' hybrid model, where employees divide their time between home and office, is here to stay. In both remote and hybrid work environments, reliance on productivity applications — such as email, virtual conferencing, instant messaging, and cloud collaboration tools — has increased, creating more diverse channels for threat exposure.

The hybrid work landscape also amplifies the risk of falling victim to well-crafted, social engineering attacks. Grappling with the risks of inevitable human error and the constant evolution of threat tactics challenges security teams with some strategic questions:

1. How can we embed security seamlessly into employees' existing workflows?
2. How can we minimize, rather than eliminate, the likelihood of human error?
3. How can we mitigate the impact of human error when it inevitably occurs?

Organizations can tackle these questions by updating how they mitigate the risks associated with their most commonly-used applications and resources.

[Remote browser isolation \(RBI\)](#) technology, which separates a user's Internet browsing from their local browser and device, shows potential to be the single most powerful way to mitigate web-based attacks. Running browsing sessions far away from local devices can protect businesses against a wide array of malicious threats — without compromising their users' accessibility and experience.

However, in practice, traditional RBI approaches have fallen short due to high costs, frustrating performance, and security exposure driven by deployment gaps.

Below, we examine the causes and consequences of these challenges, and illustrate how Cloudflare's distinct approach to browser isolation overcomes these common issues.



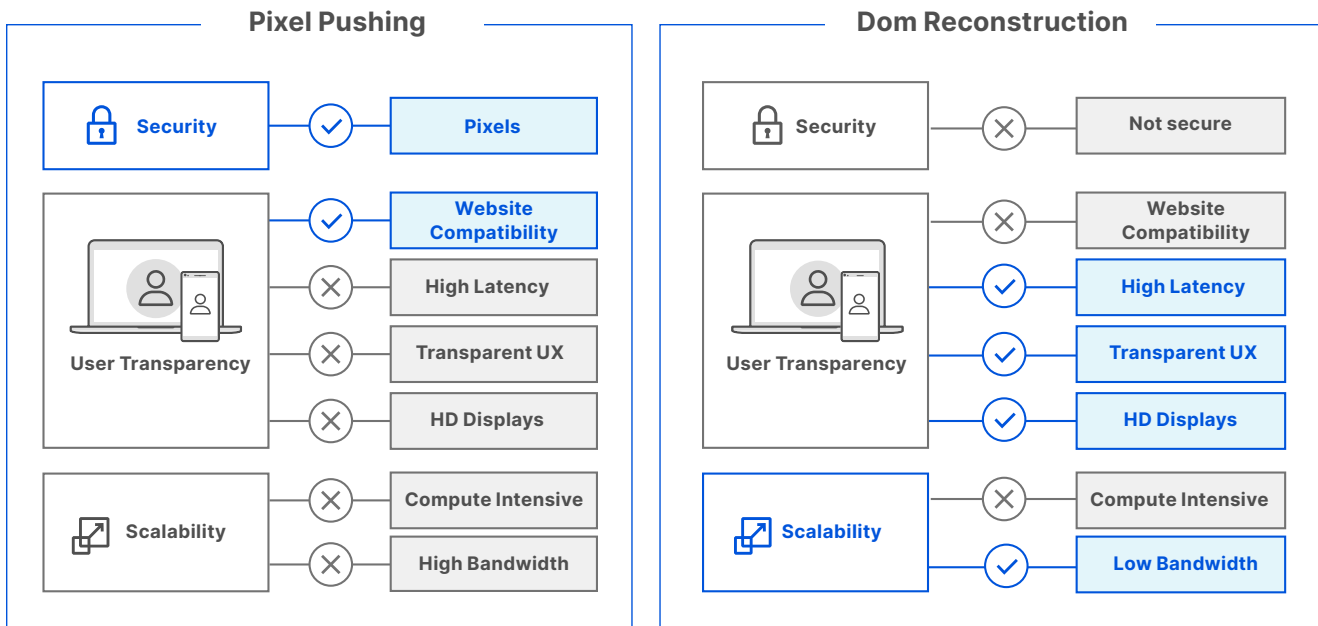
# The limitations of legacy browser isolation approaches

RBI technology provides a way to keep browsing activity secure by isolating the webpage loading process from the user and their local device. This isolation prevents malicious content from directly interacting with the user’s system, effectively thwarting web-based threats. There are primarily two RBI approaches: ‘Pixel-Pushing’ and Document Object Model (DOM) Reconstruction.





- Pixel pushing:** In this approach, the web content is rendered and processed on a remote server instead of the user’s device. The server then captures the visual representation of the webpage and sends it to the user’s device as an interactive image or video stream. This method ensures that any malicious content remains confined to the remote server, reducing the risk of infecting the user’s local system.
- DOM reconstruction:** A webpage’s Document Object Model (DOM) is a structured representation of the HTML elements on a page. DOM reconstruction involves parsing and processing web content on a remote server, which then rebuilds the webpage’s DOM to send to the user’s device. The reconstructed DOM is sanitized, ensuring that any potentially harmful scripts or content are removed before reaching the user’s device. Compared to pixel pushing, this approach does a better job of maintaining the interactivity and responsiveness of the original webpage.

While each technique offers varying benefits, both present a tradeoff between security and end-user productivity. This can create ongoing challenges when looking to deploy and scale RBI for long-term success.

## Common browser isolation technologies



## Top four challenges with common RBI methods

Pixel pushing	DOM reconstruction
<p> <b>Disruptive end-user experience:</b></p> <p>With pixel pushing technology hosted in the public cloud — or on a geographically limited private network — end users will often experience latency when they are physically distant from browser isolation data centers. This problem compounds when user traffic passes through other security tools — such as a <a href="#">secure web gateway</a> — that are not hosted in the same data centers, or that require multiple ‘passes’ through inefficiently-architected containers.</p> <p>Image streaming is also bandwidth-hungry, which can overburden network infrastructure and negatively impact user experience. In addition, pixel density increases exponentially with resolution, which means remote browser sessions (particularly fonts) on certain devices can appear fuzzy or out of focus.</p>	<p> <b>Limited security and compatibility:</b></p> <p>DOM reconstruction can sometimes result in websites rendering improperly due to its attempts to remove malicious active code, reconstruct HTML and CSS, and rebuild uncommon site architectures. Frequent changes to a site may break the ability to reconstruct it.</p> <p>While this method serves as a form of browser isolation, it still involves sending untrusted third-party code to local devices. If the service fails to detect malicious code — an ongoing risk given how dynamic the threat landscape is — endpoint devices remain vulnerable and may still be compromised.</p> <p>DOM reconstruction can also struggle to support common collaboration ecosystems like Microsoft 365 and Google Workspace.</p>
<p> <b>Poor scalability:</b></p> <p>Continuously encoding video streams of remote webpages to end-user devices is very costly in terms of the amount of compute required on the backend architecture. Pixel pushing also requires significant bandwidth, even when highly optimized.</p> <p>Due to the high resource consumption associated with this method, costs are frequently passed on to customers. This can impede the scalability of the solution to accommodate organization-wide needs. The financial burden can hinder the widespread adoption of such security measures.</p>	<p> <b>High compute costs:</b></p> <p>DOM reconstruction involves parsing and processing web content on a remote server, which then rebuilds the webpage. This process can be computationally demanding — particularly for complex or feature-rich webpages — requiring powerful servers and additional resources to manage the workload efficiently.</p> <p>While the process of sanitization ensures that any potentially harmful scripts or content are removed before reaching the user’s device, it involves advanced filtering and analysis that also increase the processing overhead and resources utilized.</p>

# Modern RBI technology delivers more scalable and transparent protection

As web browsers have become the most widely used corporate application, and with the proliferation of web-based threats, browser security has become a paramount concern for organizations across all sectors.

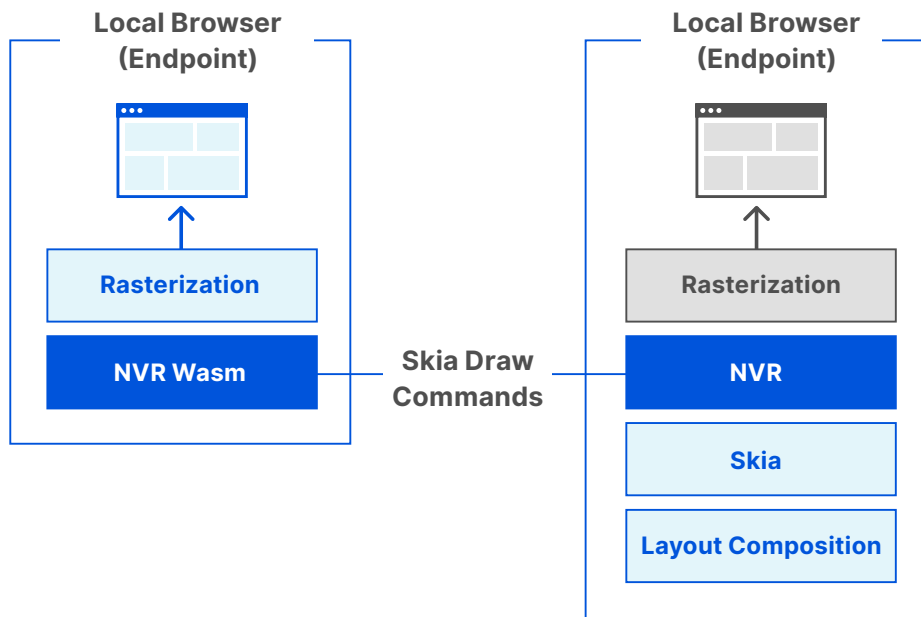
While poor end-user experiences and prohibitive costs have limited the widespread application of RBI technology in the past, Cloudflare's approach to developing and integrating RBI capabilities has successfully overcome these challenges.

Unlike bandwidth-heavy pixel pushing or fragile content-disarm and reconstruction RBI techniques, [Cloudflare Browser Isolation](#) utilizes a proprietary method called **network vector rendering (NVR)**. NVR streams safe draw commands to the device — without transmitting any malicious web page code or impacting the end user experience. This unique approach enables a more secure, transparent, and scalable service that makes RBI more accessible to and practical for organizations.

## How NVR reinvents the foundation of browser isolation

Cloudflare's RBI service is built on Chromium, and a key architectural feature of Chromium is its use of Skia — a widely-used, cross-platform graphics engine for Android, Google Chrome, Chrome OS, Mozilla Firefox, and many other browsers. All HTML5-compliant browsers can render Skia. Everything visible in a Chromium browser window, including the entire contents of the webpage window, is rendered through the Skia rendering layer.



Cloudflare's NVR technology intercepts the remote Chromium browser's Skia draw commands, tokenizes and compresses them, then encrypts and transmits them across the wire to any HTML5-compliant web browser running locally on the endpoint desktop or mobile device. The Skia API commands captured by NVR are pre-rasterization, which means they are highly compact. And since Skia is so widespread, Cloudflare's remote browser isolation works on any modern web browser.



NVR is also a more secure way to deliver a remote browsing experience. Since Cloudflare sends draw commands rather than actual website code to end-user devices, the underlying data transport is not an attack vector. This eliminates the opportunity for exploitation.

Cloudflare Browser Isolation runs a headless version of the Chromium browser, which renders all browser code at our edge, instead of on the device, to mitigate both known and unknown threats. Cloudflare can even isolate downloaded files and move them to various locations per the end-user’s needs.

**Key differentiators of Cloudflare’s NVR technology:**


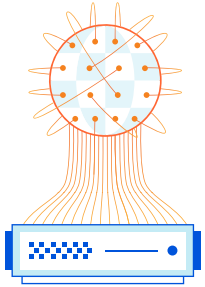

-  Streaming draw commands delivers a safer, faster, and more transparent user experience
-  Compatibility with all modern browsers based on Chromium architecture

**The benefits of using modern RBI technology**

For organizations to embrace RBI technology as a way to protect Internet browsing, the service needs to be more scalable, economically efficient, and flexible. If an organization grows their workforce, their RBI solution should be able to quickly scale without technical limitations or exponentially increasing costs.

Subpar browsing experiences impede productivity, leading to business delays or unsanctioned workarounds that ultimately diminish end-user protection. Therefore, in addition to scalability and cost efficiency, it is also critical for any remote browsing solution to feel smooth and transparent – just like local browsing. This ensures daily workflows are not disrupted.

To address the primary deficiencies caused by legacy architectures, Cloudflare has fundamentally redesigned remote browsing to be safer, faster, and more resilient. **Combining the efficiency and security of NVR with the performance and presence of Cloudflare’s global network effectively resolves many of the limitations of previous RBI approaches.**

Problem	Cloudflare's solution
<p><b>Security exposure</b></p> 	<p><b>Utilize native browser technology with no known exploits:</b> Instead of trying to decide which code to send or block, Skia commands avoid the need to send code altogether. Cloudflare's native browser technology enables the ability to only send the last step in the rendering process that draws the webpage.</p> <p><b>Provide granular control over user interactions:</b> Cloudflare Browser Isolation gives administrators the ability to control how users interact with content in the browser, including disabling copy/paste, upload/download, printing and form inputs, to minimize the risk of data loss.</p>
<p><b>Disruptive end-user experience:</b></p> 	<p><b>Harness a global edge network to reduce latency:</b> Cloudflare Browser Isolation is hosted in every data center on its global edge network, which spans 285+ cities in 100+ countries and sits within 50ms of 95% of the world's Internet users. This same infrastructure delivers ultra-low latency global DNS and CDN services while enabling seamless interaction with an array of other security solutions to provide single-pass filtering and inspection of webpages.</p> <p><b>Utilize native browser technology to increase compatibility and performance:</b> NVR technology transmits lightweight vector commands rather than pixel images or 'scrubbed' code, which requires significantly less bandwidth than other RBI methods. It also ensures that even complex and frequently updated webpages will render properly.</p>
<p><b>High cost, low scalability</b></p> 	<p><b>Utilize native browser technology to reduce costs:</b> NVR's ability to send lightweight Skia commands reduces overall compute demands on the backend infrastructure. Since the solution operates on Cloudflare's own network, server resources can be orchestrated and managed more efficiently, further reducing operational costs.</p> <p><b>Employ next-gen cloud computing to improve efficiency:</b> Cloudflare's serverless computing techniques improve on virtualization and containerization to use resources more effectively while avoiding the seconds-long cold starts that frequently affect applications hosted on the public cloud.</p>



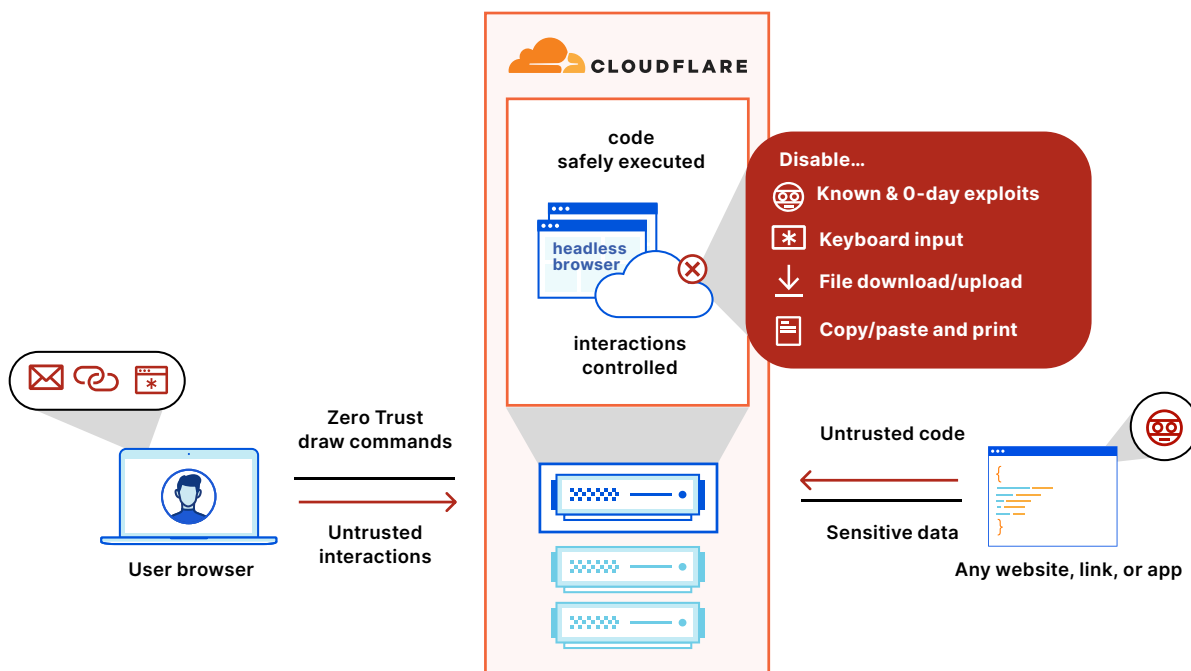
# Key use cases for modern RBI technology

## Stop multi-channel phishing attacks

The rise of phishing as one of the most popular attack vectors has driven malicious actors to develop creative ways to bypass traditional email security controls. This evolution has led to multi-channel [phishing](#) attacks, where users are targeted across multiple communication channels, such as email, web, IM, social media, cloud storage, and other frequently used collaboration tools.

With email being the most ubiquitous and most exploited application, attackers often use embedded email links as the initial means to expose users to malicious web content that can lead to account compromise or data exfiltration. As phishing attacks become more targeted and evasive, even the best trained users (and security solutions) struggle to accurately detect malicious links 100% of the time. By natively integrating next-generation browser isolation capabilities with cloud email security, Cloudflare is able to eliminate the slim, yet highly dangerous, margin of risk created by suspicious links embedded in emails.

This native functionality, known as [email link isolation](#), automatically isolates suspicious email links to prevent users from being exposed to potentially malicious web content. Keyboard inputs can also be disabled on untrusted websites, protecting users from accidentally entering sensitive information within a form fill or credential harvester.



Integrated browser isolation and cloud email security stop modern phishing threats

Email link isolation removes the manual and time-consuming effort of having to determine whether to allow or block an embedded email link when there's insufficient intelligence to categorize the link as benign or malicious. This provides a final layer of defense against multi-channel attacks by effectively allowing users to safely open any link without fear of exploitation or disruption to their workflow.

## Insulate users from malware

Organizations of all sizes and across all industries are threatened by [malware](#) in all its various forms: viruses, worms, Trojans, rootkits, ransomware, and more. Malware is constantly evolving, and each attack (or lack of adequate response to one) can lead to larger attacks. In fact, Gartner notes, "These attacks can take weeks or months to unfold, leaving malware deeply embedded in systems throughout the organization. When this work is complete, the ransomware is deployed to encrypt critical data, including the backup store, if it's accessible on the network."<sup>1</sup>

While Cloudflare Browser Isolation can effectively protect against all forms of web-based malware attacks, native integration across other Zero Trust services can help extend protection to non-isolated sites. Additional techniques for blocking malware include:



- **Email link isolation**, as described earlier, insulates email users from malicious web content and removes the IT burden of managing complex email allowlist or blocklist policies.
- **DNS filtering** from [Cloudflare Gateway](#) provides another layer of security for organizations to automatically block risky or malicious websites and filter out harmful content.
- **HTTPS inspection** (also known as SSL inspection or TLS inspection) for [Cloudflare Zero Trust](#) customers increases visibility into malware encrypted in HTTPS. This process checks encrypted web traffic by using the same technique as an on-path attack on the network connection. HTTPS inspection leverages the power of Cloudflare's DNS and HTTP telemetry and threat detection models to protect organizations from 'hidden' malware.

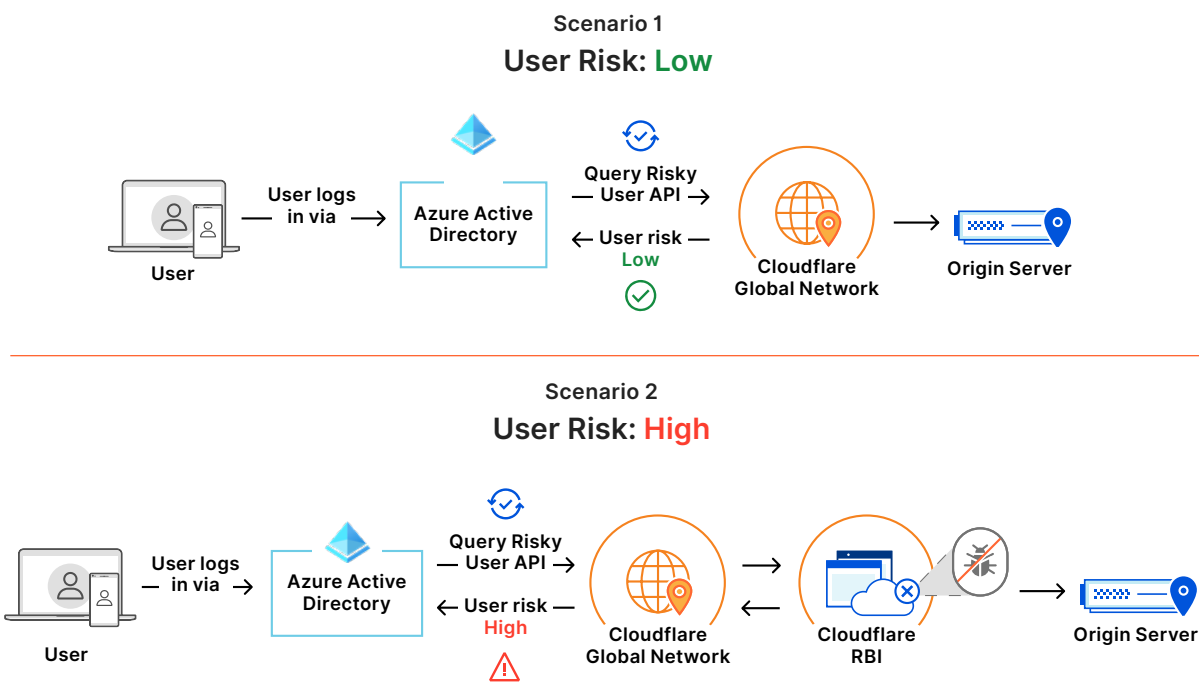
1. Simpson, Nik, and Blair, Ron. "Detect, Protect, Recover: How Modern Backup Applications Can Protect You from Ransomware," Gartner, 14 December 2022.

## Isolate contractors and high-risk users

Moving away from the [castle-and-moat](#) security model, to a fully distributed, perimeterless model with controls delivered in the cloud requires security checks for every user accessing every resource. However, certain users can be deemed riskier than others based on the nature of their employment — i.e., contractors, suppliers, and other third parties — and other contextual factors – i.e., a history of risky sign-in behavior, use of unmanaged devices, or geography.

Cloudflare Browser Isolation can isolate connections to critical resources and applications via hyperlinks — all without installing any software on user devices. Then administrators can build data protection rules preventing risky user actions within these isolated browser-based apps. This clientless model makes it easy to scale isolation policies to employees, contractors, or third parties, even on unmanaged devices.

For joint Microsoft Azure Active Directory customers, Cloudflare also [offers](#) a **low-risk way to provide access to high-risk resources and applications**. Microsoft Azure Active Directory (Azure AD), classifies users into low, medium and high-risk users based on many data points. Cloudflare’s RBI integration adds an extra layer of security by isolating high-risk users (based on Microsoft AD signals) to browser isolated sessions.



Add an extra layer of security by isolating high risk users (based on AD signals) via Cloudflare Browser Isolation

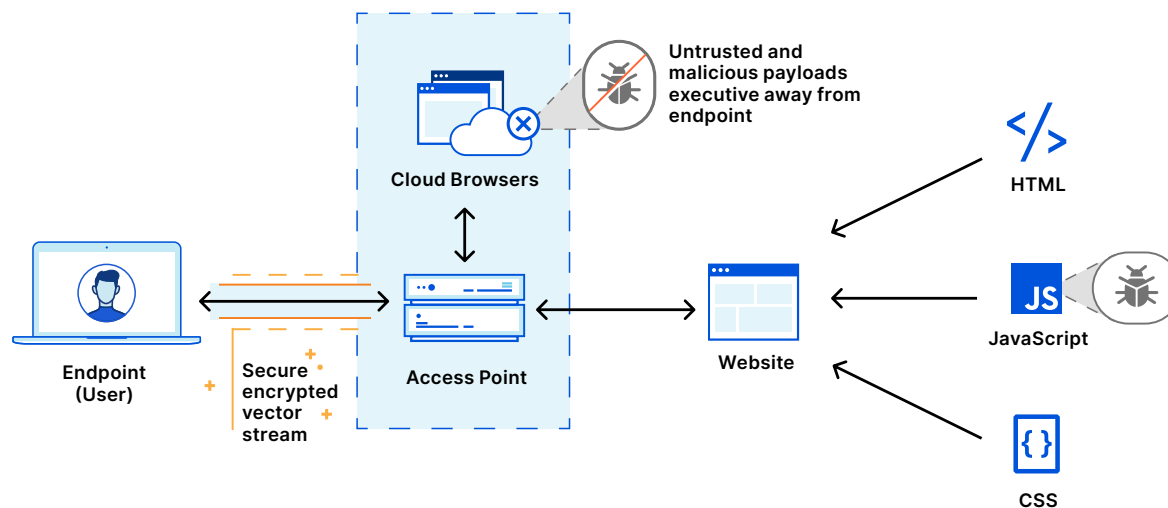
When a user is classified as high-risk on Azure AD, Cloudflare uses this signal to automatically isolate their traffic with our Azure AD integration. This means that a high-risk user can access resources through a secure and isolated browser. Users can still move from one risk group to another based on their activities; if the user were to later move from being considered high-risk to low-risk, they would no longer be subjected to the isolation policy applied to high-risk users.

## Minimize the risk of zero-day browser vulnerabilities

Like all software, web browsers can have security vulnerabilities for attackers to exploit. In particular, the volume of browser-based zero-day vulnerabilities exploited in the wild has been rising in recent years.

For example, in December 2022, Google announced its ninth [zero-day exploit](#) of the year — an emergency Chrome 108 update to patch a vulnerability (CVE-2022-4262) in the browser. The high-severity [type confusion](#) flaw generally leads to browser crashes after successful exploitation, and threat actors could also exploit them for arbitrary code execution. Plus, earlier in 2022, Mozilla also released emergency updates for its Firefox browser to address a zero-day exploit that could lead to remote code execution, data corruption, and system crashes.

Although browser risks cannot be completely eliminated, organizations can reduce the risk of zero-day browser exploits by patching browsers remotely — instead of relying on end-user or IT administrator intervention.



*Protect users browsing the Internet from zero-day threats*

With Cloudflare Browser Isolation, IT and security teams do not need to ask end-users to manually update their browser, enable updates via mobile device management, or install other patches that demand their attention and time. Cloudflare automatically deploys patches to remote browsers, and any traffic to an isolated website is automatically served from the patched remote browser.

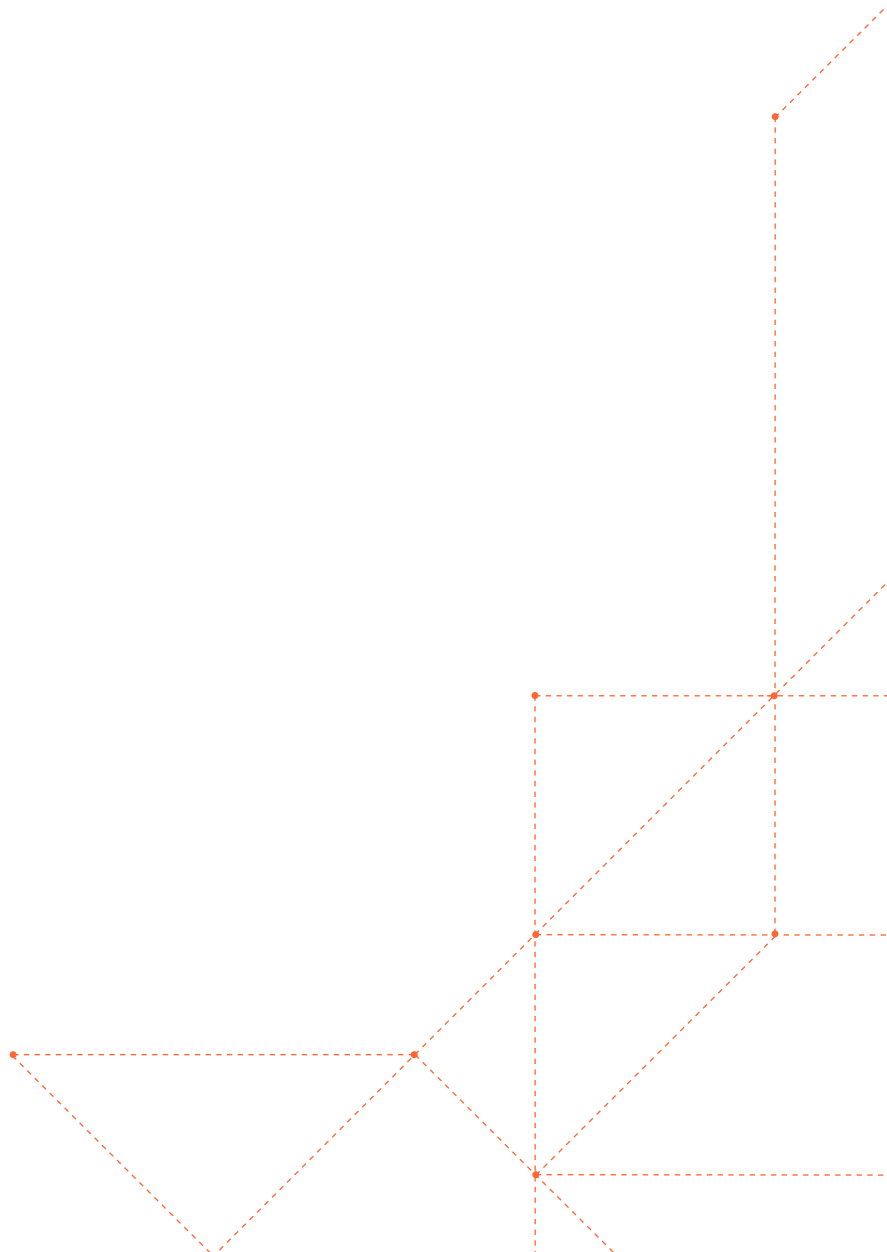
Cloudflare's additional techniques to protect against zero-day threats while users browse the Internet include:

- Steering Internet traffic over an encrypted tunnel to a nearby Cloudflare data center for inspection and filtration
- Inspecting and filtering traffic based on Cloudflare's network intelligence, antivirus scanning, and threat feeds
- Executing all website code in a remote browser at Cloudflare's edge to protect unpatched devices from threats inside the unknown website

# Conclusion

Zero Trust is an approach to information security in which no user, web traffic, application, or device is trusted by default. A Zero Trust security model assumes that even though a user has safely loaded a website 99 times, the website might be compromised on the 100th time. Browser isolation applies this “never trust” mindset to Internet browsing: no web code or interactions should be trusted to run on local devices by default.

To learn more about Cloudflare Browser Isolation, and how it can help you achieve Zero Trust browsing, visit [cloudflare.com/products/zero-trust/browser-isolation/](https://cloudflare.com/products/zero-trust/browser-isolation/).



# References

1. Simpson, Nik, and Blair, Ron. "Detect, Protect, Recover: How Modern Backup Applications Can Protect You from Ransomware," Gartner, 14 December 2022.

## Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved



© 2023 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

1 888 99 FLARE | [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [www.cloudflare.com](http://www.cloudflare.com)