CLOUDFLARE

SOLUTION BRIEF

Isolate Suspicious Email Links

Neutralize malicious email links while ensuring disruption-free productivity

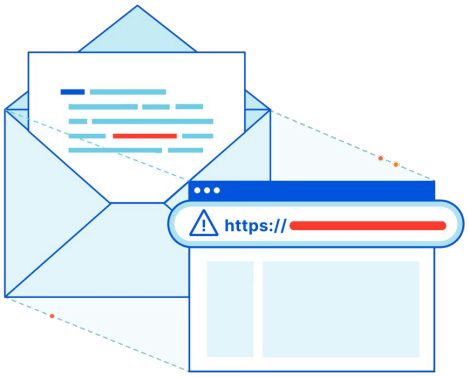
Safely click unknown links with email link isolation

Challenge: Protecting against deceptive email links

As modern phishing attacks become more evasive and sophisticated, even the best trained users (and security solutions) struggle to accurately detect malicious links 100% of the time. This results in:

- **Greater risk**: Allowing unknown email links to be clicked by end users presents additional opportunities for exploitation.
- **Workflow disruption**: Having to block or investigate unknown email links can delay normal business activity.
- **More time and effort:** Investigating unknown email links and false positives can consume a significant amount of time and resources.

With email being the #1 most used and most exploited business application, attackers often use embedded email links as a means to expose users to malicious web content that can lead to account compromise or data exfiltration.



Solution: Integrated cloud email security + remote browser isolation

Email link isolation from Cloudflare Area 1 automatically applies **adaptive isolation to unknown email links** to insulate users from malicious content and remove the burden of managing complex policies.

Opening suspicious email links in an isolated browser neutralizes any potential malware by running all code in the cloud, far away from the user and their device.

Key benefits:

Reduce risk
Minimize attack surface and exposure by insulating your users from untrusted web content and multichannel phishing threats.

Drive productivity
Ensure uninterrupted productivity for end users by delivering the most seamless, low-latency browser isolation experience on all device types.

Remove complexity
Reduce false positives while saving IT and SecOps time by automatically allowing all unknown and suspicious links to be clicked safely.

Email link isolation from Cloudflare Area 1

Defend against new multichannel threats

Threat actors are increasingly targeting individual users through multiple channels of communication (email, web, SMS, and more), often leveraging email as the initial attack vector. These multichannel phishing attacks commonly employ malicious email links and use evasive tactics that bypass traditional security controls. Examples include:

- **Deferred phishing**: An initially benign link within an email is later weaponized to point to a malicious destination after delivery.
- **Cloud service phishing**: Dangerous HTTPS links closely resemble common cloud services (e.g. Google Drive, Box).

> "We started using Cloudflare Zero Trust services with Browser Isolation to help provide the best security for our customers' data and protect employees from malware. It worked so well I forgot it was on."
>
> **Jonathan Lister Parsons**
> CTO, PensionBee

Minimize risk without compromising user experience

By integrating next-generation browser isolation capabilities built on our unique **Network Vector Rendering (NVR)** technology, Area 1 is able to deliver a **seamless**, **secure**, **and scalable** solution for isolating suspicious email links.

Unlike bandwidth-heavy techniques, NVR streams safe draw commands to the device. This helps eliminate the risk of untrusted code running on the device, or impacting the end-user experience.

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

How email link isolation works

1. Email Analysis

Inbound email is analyzed using Cloudflare Area 1 threat intelligence to classify as malicious, benign, or suspicious

2. Link Isolation

If classified as suspicious, link is rewritten to a custom Cloudflare prefix URL

3. Email Delivery

Email is delivered to the intended inbox

4. Time-of-Click

When user clicks on rewritten link, system does a time-of-click analysis to determine link classification

5. Interstitial Page

If link is still classified as suspicious, then interstitial page is displayed to warn users and offer browser isolation

6. Isolated Browsing

When user clicks 'Open in Remote Browser', an isolated browser session loads in the closest PoP on the Cloudflare network

The power of extending Zero Trust protection to email security

Secure hybrid work with Zero Trust

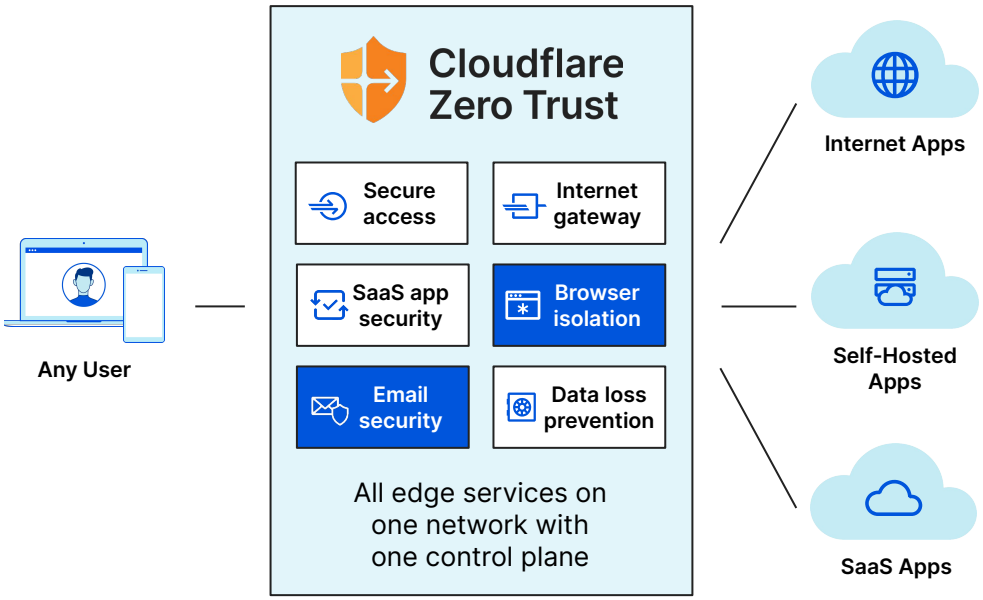
Cloudflare Zero Trust increases visibility, eliminates complexity, and reduces risks as remote and office users connect to corporate applications and the public Internet.

Cloudflare offers the most comprehensive Zero Trust approach by providing visibility and control across all internal and external network, web, and email traffic; delivering layered security that is easily tailored to each organization.

Cloud email security: Core to Zero Trust

Cloudflare Area 1 email security enhances Zero Trust by removing implicit trust from email to preemptively stop phishing and business email compromise (BEC) attacks.

Never trust any sender, even if internal. Instead, ensure all user traffic, including email, is verified, filtered, inspected, and isolated from Internet threats. Area 1 is integrated across Cloudflare's Zero Trust platform, delivering a more seamless set of solutions.



VPN replacement
simplify and secure connecting any user to any resource

Internet protection
keep your data safe from threats over any port and protocol

Streamline SaaS security
visibility and control of applications including email

Security modernization
improved productivity, simpler operations, reduced attack surface

Discover which attacks your current email security systems miss - at no cost and no impact to your end users. Request a complimentary Phishing Risk Assessment today.