# Cloudflare Remote Browser Isolation Overview

*DISA Technical Exchange Meeting*
*11-June-2024*

- *John Kaden, Government Programs*
- *Scottie Ray, Senior Solutions Architect*
- *Tim Obezuk, Zero Trust Specialist Solutions Engineer*
- *Chase Disher, Product Manager*

# Agenda

Introductions

Cloudflare Network

Browser Isolation Overview

Demonstration

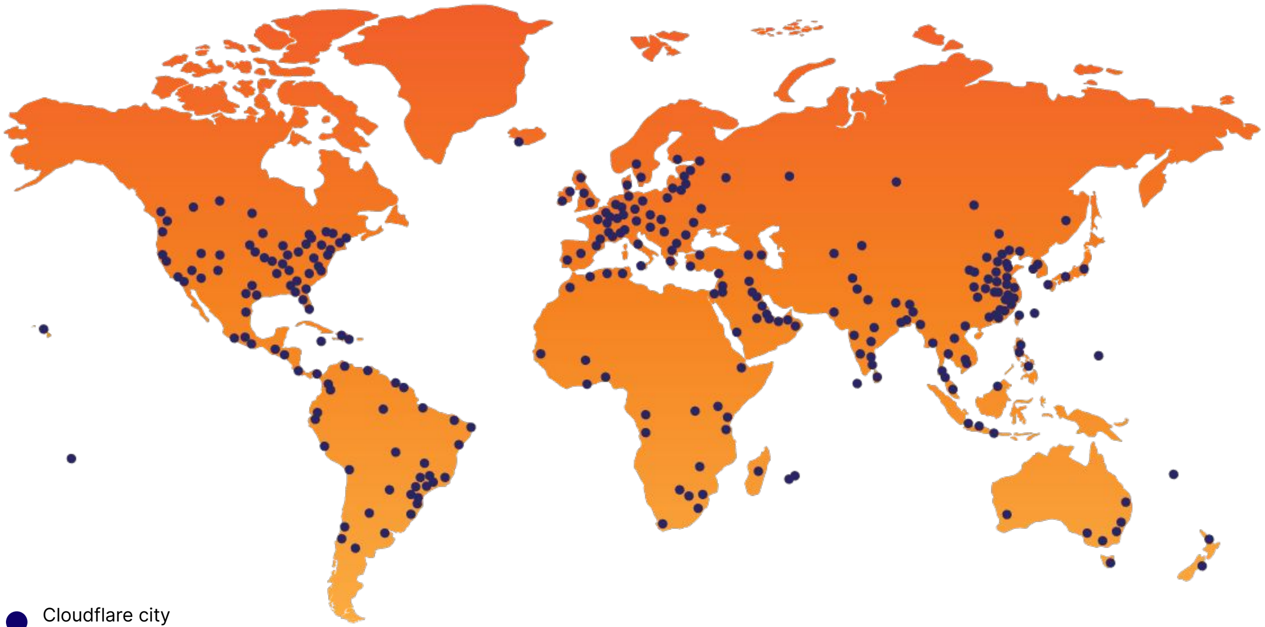
Questions

Closing

DISA

CLOUDFLARE

# Cloudflare Network Evolution



● Cloudflare city
(As of Q1 2024)

## 310

cities in 120+ countries, including mainland China

## 13,000

networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

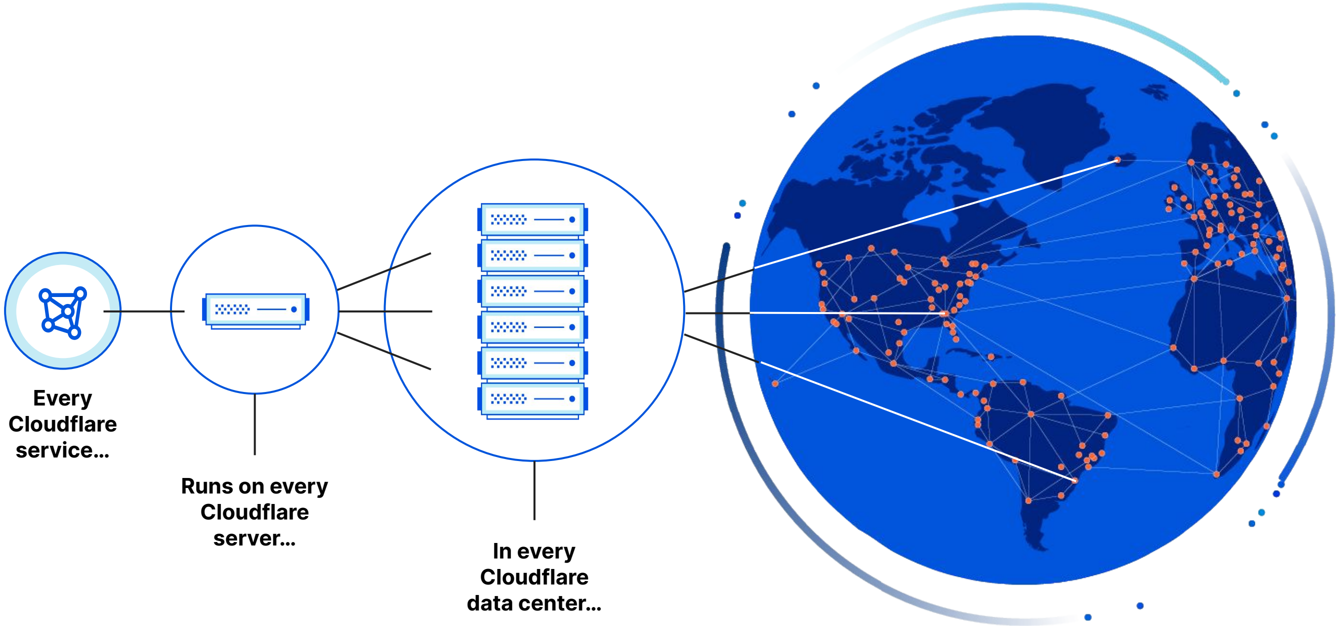
## 248 Tbps

global network edge capacity, consisting of transit connections, peering and private network interconnects

## ~50 ms

from 95% of the world's Internet-connected population

# Every service runs on every server, in every FedRAMP PoP



Every Cloudflare service…

Runs on every Cloudflare server…

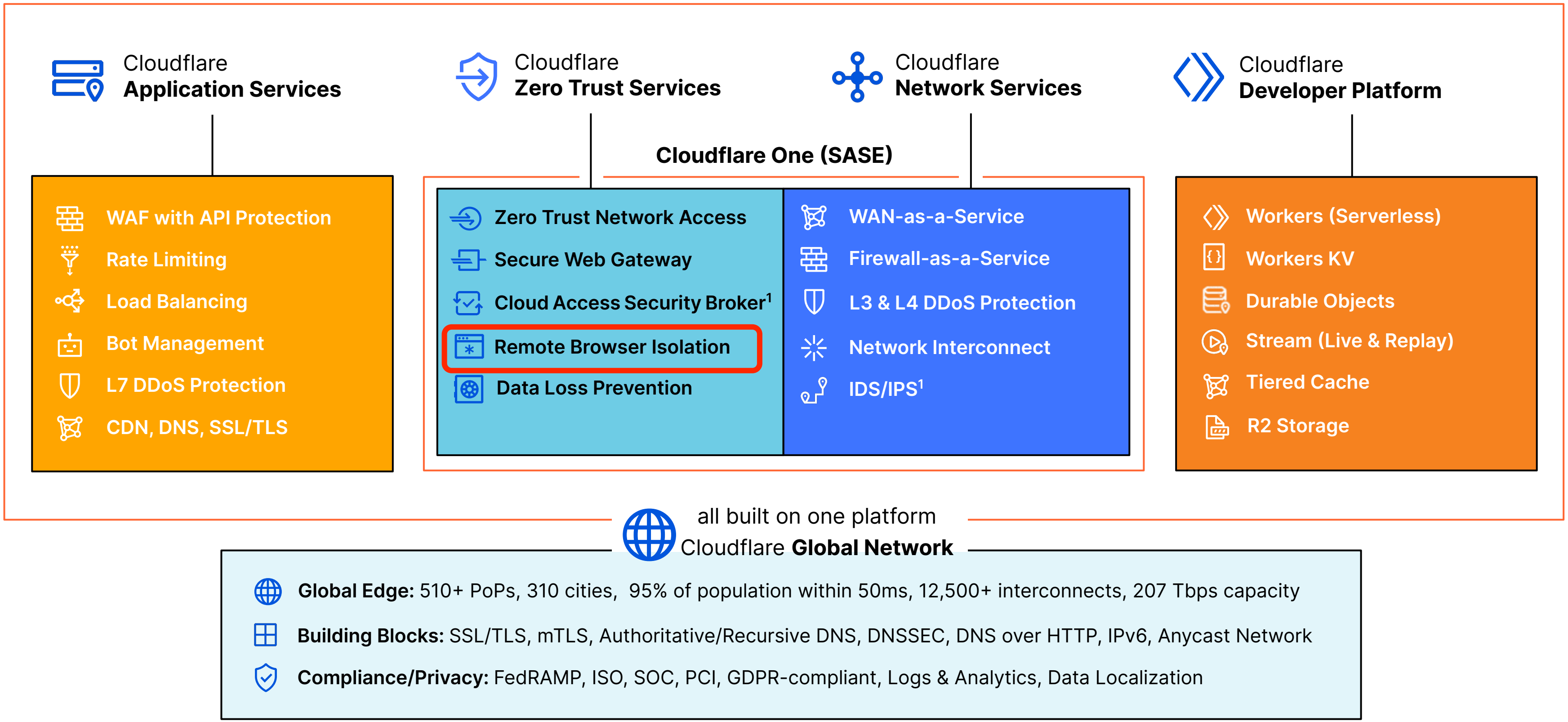
In every Cloudflare data center…

Across 510+ PoPs in 100+ countries

**Users connected via Anycast Routing**

means requests can automatically be routed to a variety of locations (“nodes”) without the end user or admin having to pick a destination

# Remote Browser in the Cloudflare Platform



Cloudflare **Application Services**

- WAF with API Protection
- Rate Limiting
- Load Balancing
- Bot Management
- L7 DDoS Protection
- CDN, DNS, SSL/TLS

**Cloudflare One (SASE)**

Cloudflare **Zero Trust Services**

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker[1]
- Remote Browser Isolation
- Data Loss Prevention

Cloudflare **Network Services**

- WAN-as-a-Service
- Firewall-as-a-Service
- L3 & L4 DDoS Protection
- Network Interconnect
- IDS/IPS[1]

Cloudflare **Developer Platform**

- Workers (Serverless)
- Workers KV
- Durable Objects
- Stream (Live & Replay)
- Tiered Cache
- R2 Storage

all built on one platform
Cloudflare **Global Network**

**Global Edge:** 510+ PoPs, 310 cities,  95% of population within 50ms, 12,500+ interconnects, 207 Tbps capacity

**Building Blocks:** SSL/TLS, mTLS, Authoritative/Recursive DNS, DNSSEC, DNS over HTTP, IPv6, Anycast Network

**Compliance/Privacy:** FedRAMP, ISO, SOC, PCI, GDPR-compliant, Logs & Analytics, Data Localization

[1] Future FedRAMP inclusion and/or currently in Beta
(updated Jul  2023)

# Browser Isolation

# Overview

*Tim Obezuk*

Update

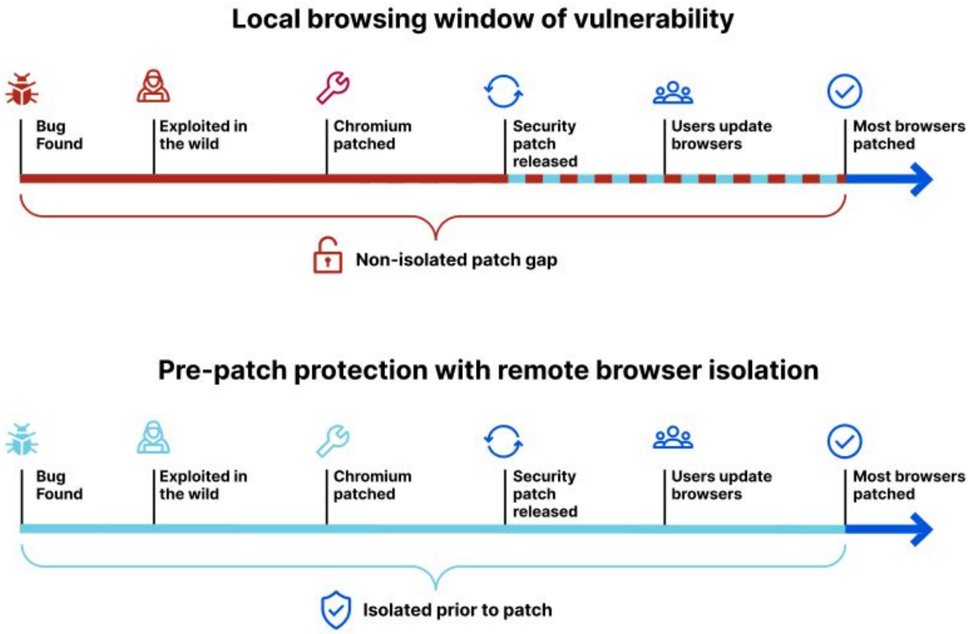
# 8 high-severity Chrome zero day vulnerabilities so far in 2024

The web is a constantly expanding attack surface.

36% DoD of attacks are browser based.

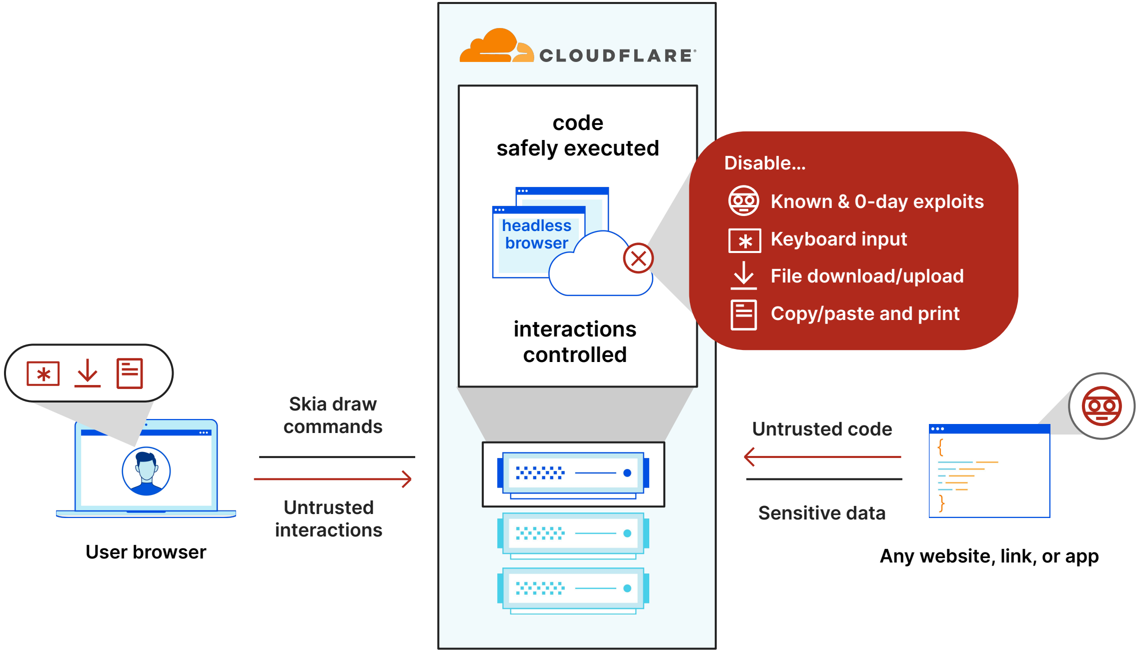
Web browsers require constant patching.

Cloudflare Browser Isolation protects users from browser-based threats pre-and-post patch.

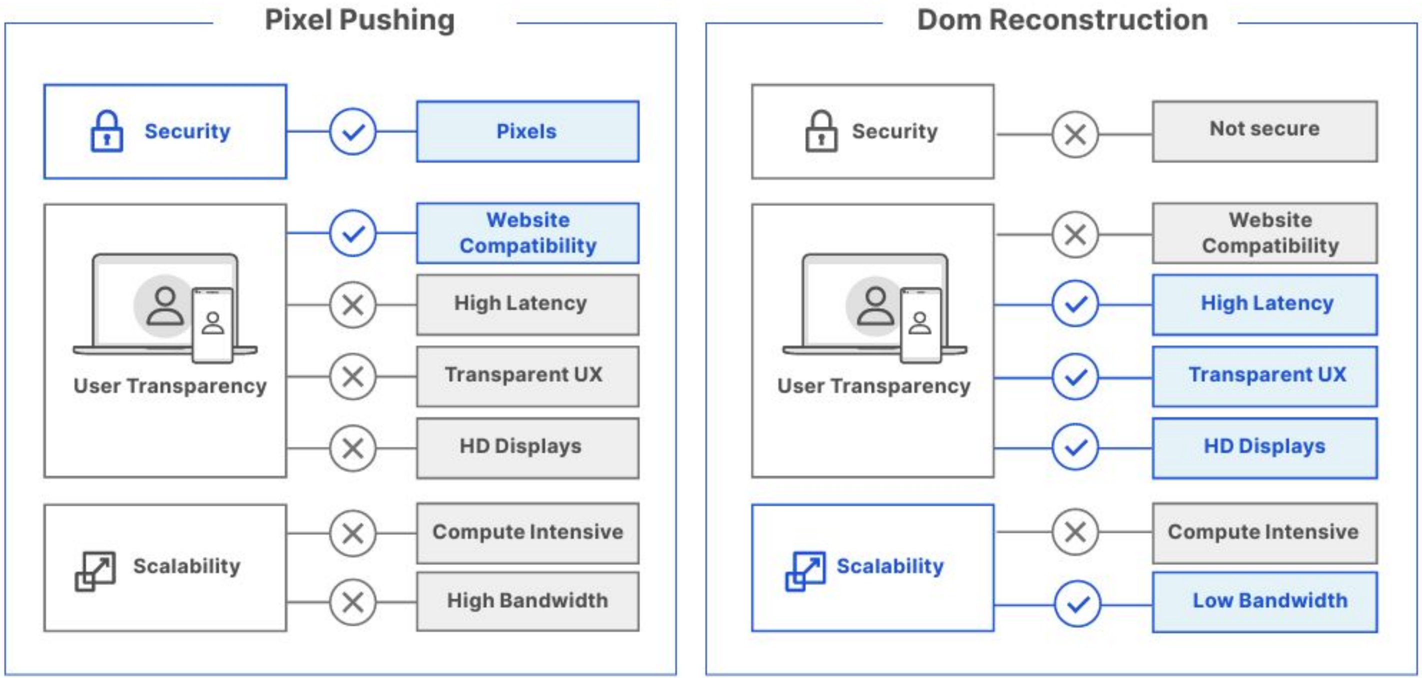


# Zero Trust Browsing: Threat defense

- Insulate users from untrusted web content
- Unique, superior **Network Vector Rendering (NVR)** technology
- Low-latency, high-resolution rendering using Network Vector Rendering (NVR)
- Compatible with all major browsers



# Legacy Browser Isolation Technologies



## Pixel Pushing

| | | |
|---|---|---|
| Security | ✓ | Pixels |
| User Transparency | ✓ | Website Compatibility |
| | ☒ | High Latency |
| | ☒ | Transparent UX |
| | ☒ | HD Displays |
| Scalability | ☒ | Compute Intensive |
| | ☒ | High Bandwidth |

## Dom Reconstruction

| | | |
|---|---|---|
| Security | ☒ | Not secure |
| User Transparency | ☒ | Website Compatibility |
| | ✓ | High Latency |
| | ✓ | Transparent UX |
| | ✓ | HD Displays |
| Scalability | ☒ | Compute Intensive |
| | ✓ | Low Bandwidth |

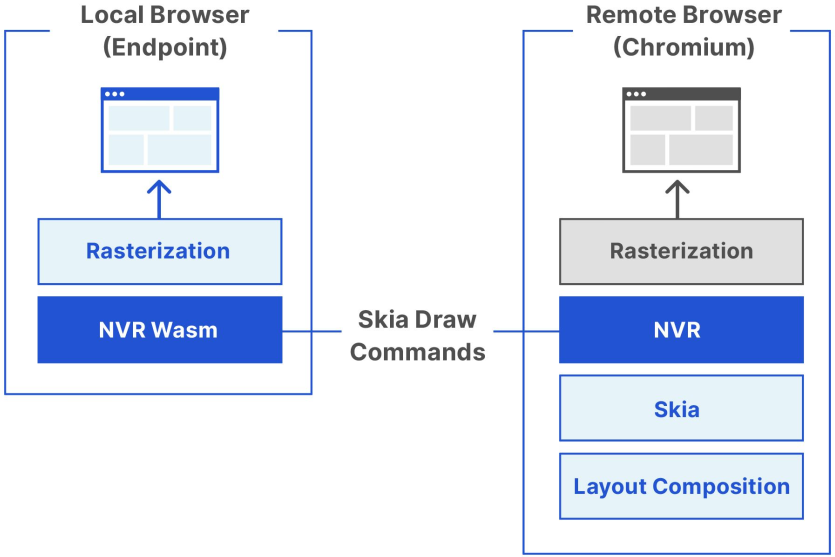
# Secure & Performant Remote Browsing Architecture

Remote Chromium-based remote browser

Local HTML5 client accessed via existing browser

Vectors over the wire, insulated from active website content

Malware isolated to isolated container



*Patented technology US10452868B1*

# Network Vector Rendering Advantages

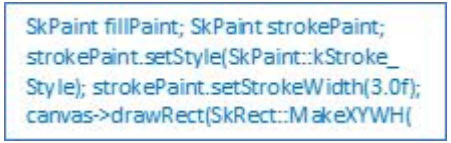
**Security**
Sanitized SKIA instructions sent to WASM client
Underlying website source is never sent to endpoints

**Compatibility**
No website compatibility issues
Future proofed for emerging website technologies

**Performance**
No encoding latency, near-native redraw performance

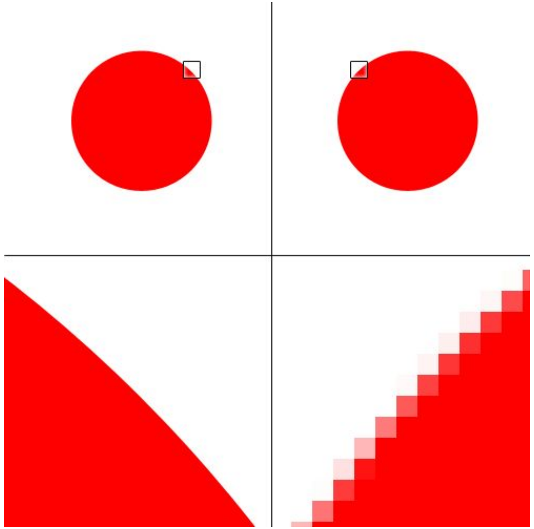
**Bandwidth**
Lower bandwidth than pixel pushing and local browsing

**Clientless**
Supports existing HTML5 compatible browser on workstation



```
SkPaint fillPaint; SkPaint strokePaint;
strokePaint.setStyle(SkPaint::kStroke_
Style); strokePaint.setStrokeWidth(3.0f);
canvas->drawRect(SkRect::MakeXYWH(
```

*Skia code fragment*



# Integration & Deployment Models

### Existing user browser

Chrome / Edge

Firefox

Safari

*Any modern HTML5 browser*

### Forward proxy

Proxy Connect Endpoint (PAC file)

Endpoint Client

Layer 3: IPsec / GRE / PNI

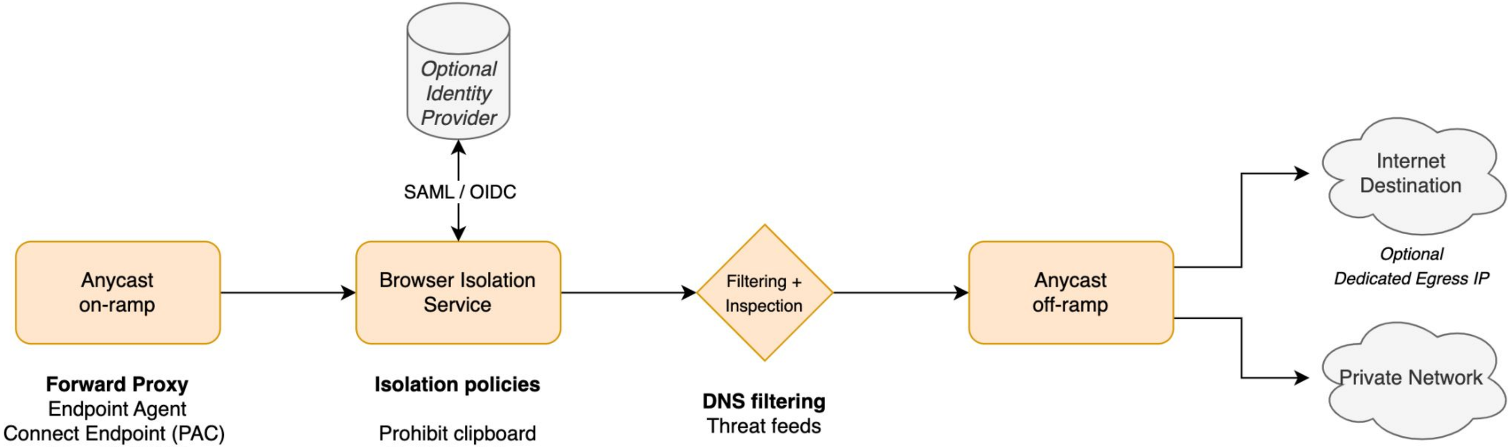
### Reverse proxy

Prefixed URL

Identity-aware App Proxy

Email links via MX record

# Life of an Isolated Request



*Optional Identity Provider*

SAML / OIDC

Anycast on-ramp

Browser Isolation Service

Filtering + Inspection

Anycast off-ramp

Internet Destination

*Optional Dedicated Egress IP*

Private Network

**Forward Proxy**
Endpoint Agent
Connect Endpoint (PAC)
IPsec/GRE/PNI

**Reverse Proxy**
Agent
PAC File
IPsec/GRE/PNI
MX Record

**Isolation policies**

Prohibit clipboard
Prohibit printing
Prohibit file transmission
Prohibit keyboard input

**DNS filtering**
Threat feeds

**Network filtering**
Protocol detection

**HTTP filtering**
Application / Content Categorization
Data Loss Prevention
Antivirus scanning

**Logging**
SIEM integration
Push to Cloud Storage

**Private Connectivity**

Software tunnel
IPsec
GRE
PNI
Physical Appliance

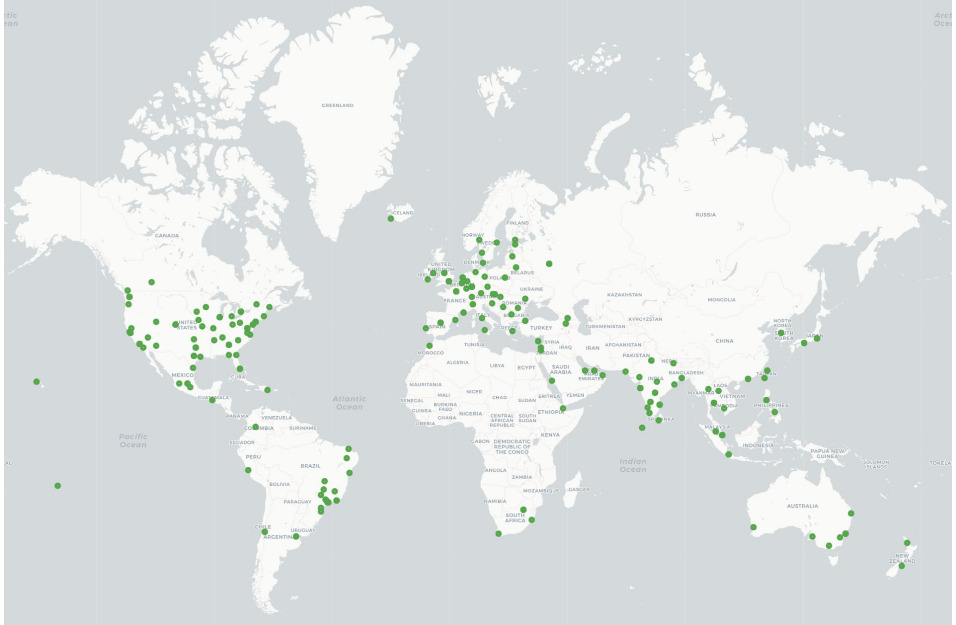
# Global Chromium Isolation Chamber

**Low latency** and **local** by default

Users can connect to remote browsers in any location, from **any location**

Scales **globally**, minimizing latency

Ephemeral Chromium containers executed in globally distributed **KVM** infrastructure



*Real world snapshot of RBI locations served - June 7, 2024*

# Roadmap

**2024 H2**

### Browser Extension

Support phish-resistant MFA to internal applications through a browser extension

### Isolate traffic based on on-ramps

Additional controls to all isolation policies based on the on-ramp intro the edge (e.g. WARP vs. clientless)

### Enhanced Logging

Provide additional monitoring capabilities around user actions and policy enforcement in the dashboard

### Disable Screenshots

Prevent users from taking screenshots of sensitive data within protected applications

### Extension Allowlist

Whitelist extensions in the browser

**2025 H1**

### DLP Integrations

Allow users to apply DLP policies which trigger isolation based on response data

### Sensitive Data Obfuscation

Mask or redact sensitive information in-line based on DLP profile detection

# Demonstration

# Questions

# Appendix

## Resources

Blog: RBI Technical Deep Dive

Whitepaper

Developer Documentation

Demo Access

## Contacts

John Kaden, johnk@cloudflare.com
Director, Federal Programs

Tim Obezuk, tobezuk@cloudflare.com
Specialist Zero Trust Solutions Engineer

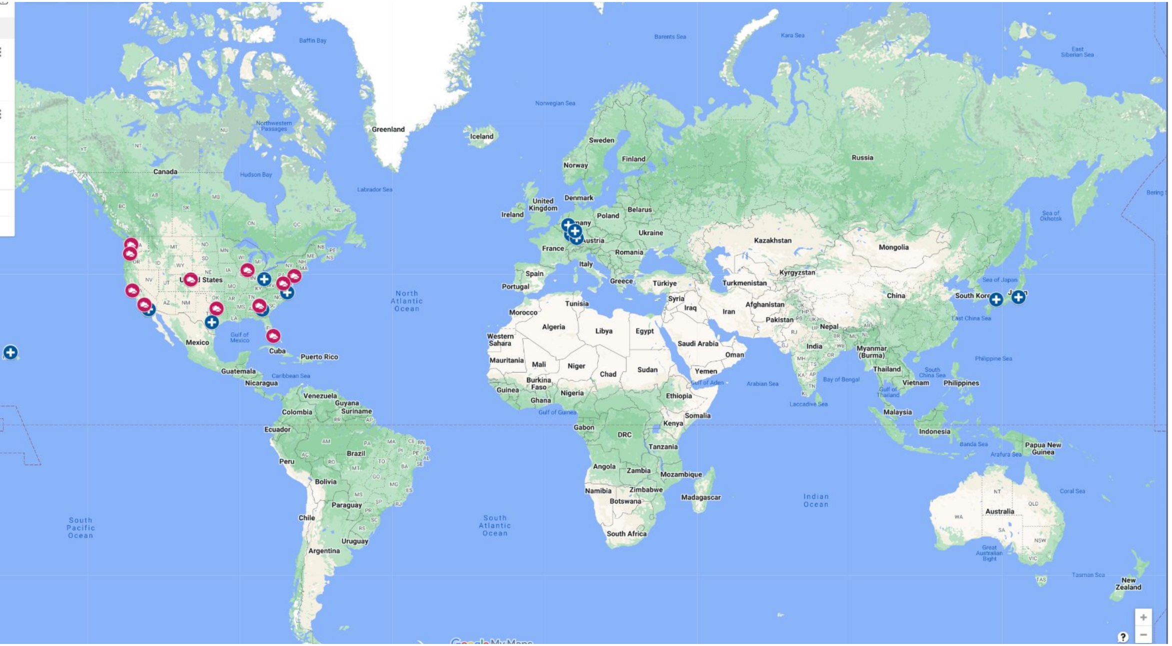
Chase Disher, cdisher@cloudflare.com
Product Manager, Zero Trust Solutions

Abe Carryl, abe@cloudflare.com
Group Product Manager, Zero Trust Solutions

Scottie Ray, scottie@cloudflare.com
Public Sector Solutions Architect

Tim Kroeger, tkroeger@cloudflare.com
Sr. Manager, Public Sector Engineering & Incubation

# IAP Locations Proximity to Cloudflare PoPs



| IAP Proximity to Cloudflare PoP | |
|---|---|
| Warner Robins (GA) | Atlanta, GA |
| Columbus (OH) | Columbus, OH |
| San Antonio (TX) | San Antonio, TX |
| North Island (CA) | San Diego, CA |
| Pentagon (DC) | Reston, VA |
| Hampton Roads (VA) | Norfolk, VA |
| Yokota (Japan) | Tokyo, JP |
| Ramstein (Germany) | Dusseldorf, DE |
| Stuttgart (Germany) | Frankfort, DE |
| Hickam (HI). | Honolulu, HI |

CLOUDFLARE

# Area 1 - Email Link Isolation

## Area 1 - Email Link Isolation

How

Area 1 Email Link Isolation *via* Remote Browser Isolation (RBI)

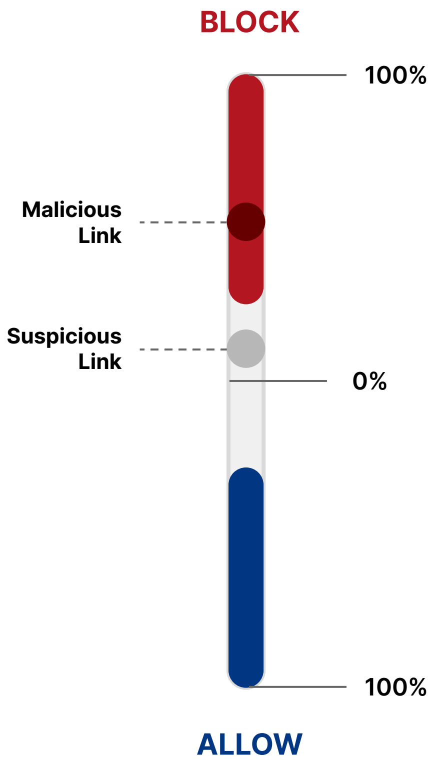
What

# To block or not to block...

Organizations struggle to efficiently handle suspicious/unknown email links without compromising security or productivity

**Block** and potentially obstruct legitimate business activity

**Allow** and potentially expose the user to malicious content



# Which leads to...

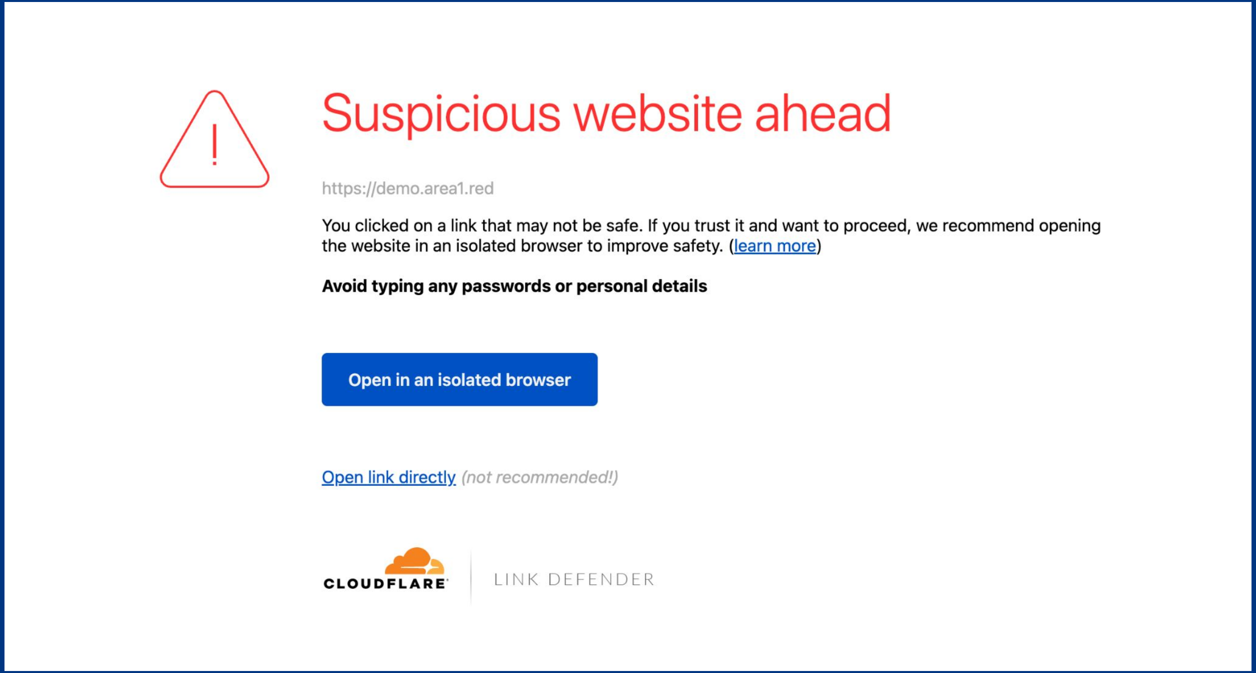
## Greater risk:

- **Multi-channel phishing attacks** that target users via email and web
- **Deferred phishing attacks** that weaponize an email link post-delivery

## More effort:

- Manually managing policies and exceptions
- Manually investigating suspicious links and false positives

# Area 1 - Email Link Isolation



Suspicious website ahead

https://demo.area1.red

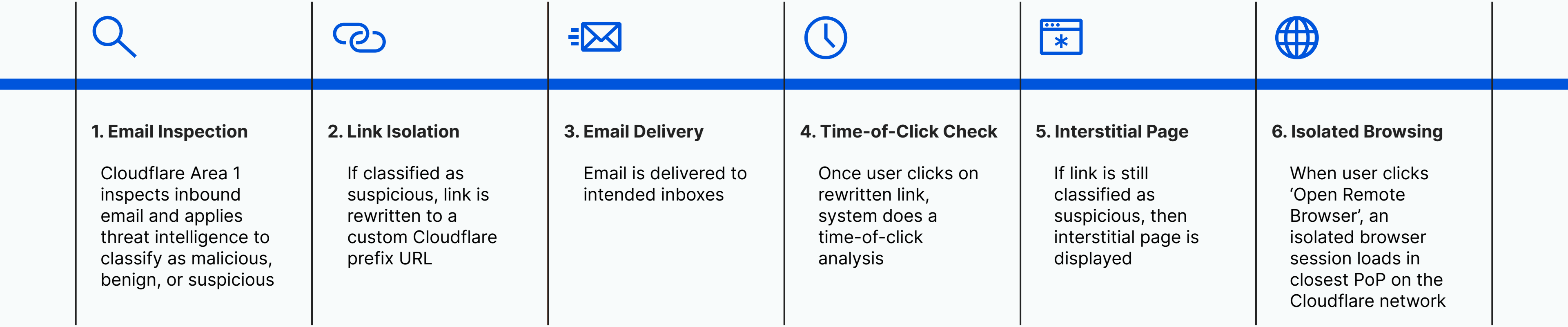
You clicked on a link that may not be safe. If you trust it and want to proceed, we recommend opening the website in an isolated browser to improve safety. (learn more)

**Avoid typing any passwords or personal details**

Open link directly *(not recommended!)*

AREA 1 - EMAIL LINK ISOLATION

# Email sequence



### 1. Email Inspection

Cloudflare Area 1 inspects inbound email and applies 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 intended inboxes

### 4. Time-of-Click Check

Once user clicks on rewritten link, system does a time-of-click analysis

### 5. Interstitial Page

If link is still classified as suspicious, then interstitial page is displayed

### 6. Isolated Browsing

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