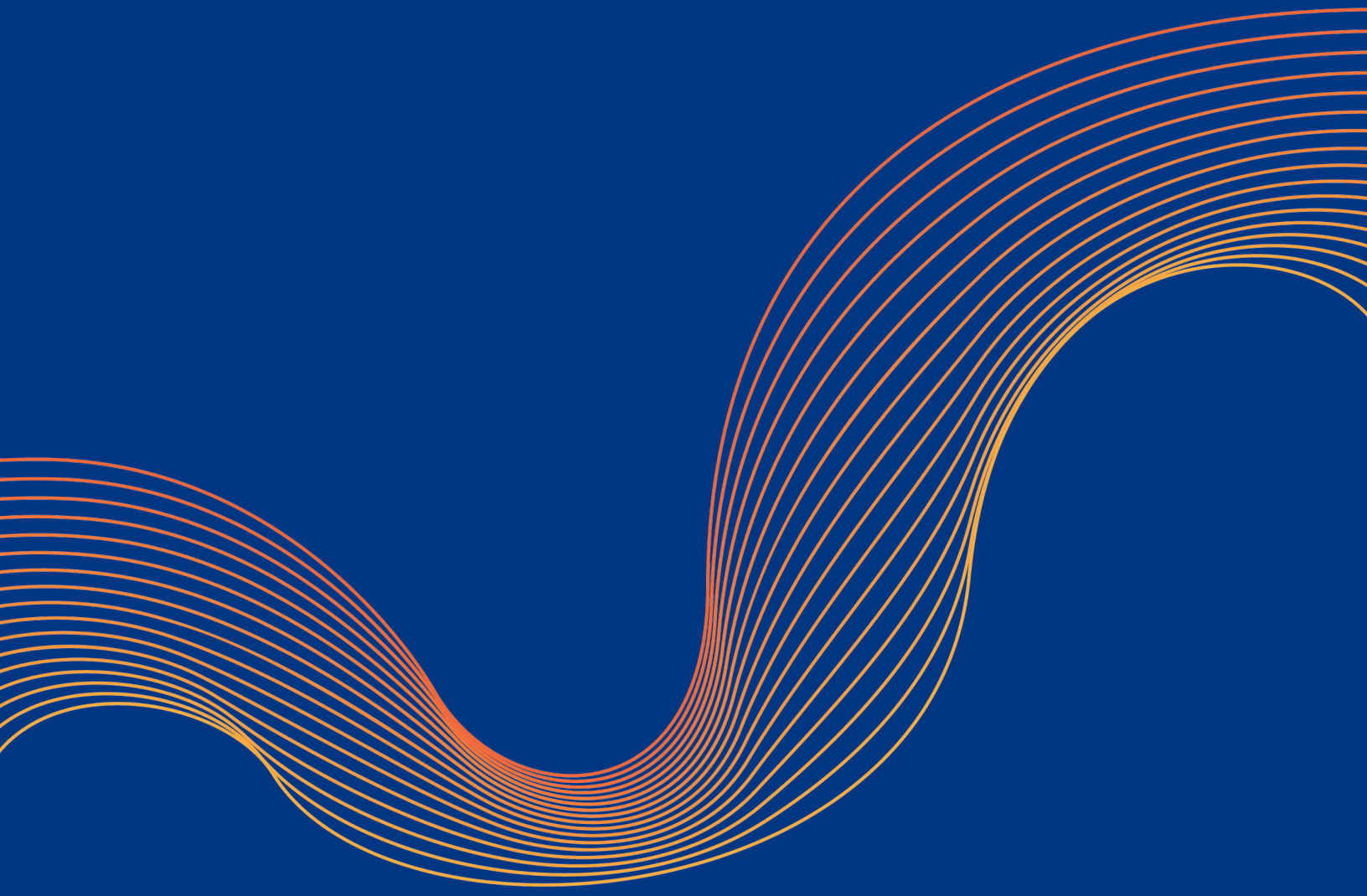
CLOUDFLARE

Problemi comuni di isolamento del browser e come superarli

Il punto di incontro tra la navigazione in Internet e la sicurezza Zero Trust



+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

INDICE

Introduzione 3

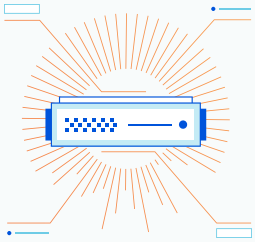
Problemi delle strategie comuni di isolamento del browser 3

- Cattura della schermata in streaming dell'attività di navigazione dal cloud 4
- Scomposizione dei siti Web nel cloud e rimozione di codice dannoso 5
- Isolamento dell'attività di navigazione in una macchina virtuale su dispositivo 6
- Questi problemi iniziali ne creano di altri 7

Un approccio migliore all'isolamento del browser in remoto 7

- Cloudflare rende la navigazione remota più conveniente e da meno problemi all'utente finale 8
- Network Vector Rendering offre migliori esperienze per gli utenti finali e colma le falle nella sicurezza 9

Scopri di più e inizia subito 9



Introduzione

I team IT e di sicurezza hanno buone ragioni per non fidarsi di Internet pubblico. Phishing e malware hanno rappresentato il 39% di tutte le violazioni dei dati nel 2020, secondo un rapporto di Verizon. Uno studio di Forrester Consulting commissionato da Cloudflare ha inoltre rilevato che, sempre nel 2020, il 61% delle aziende con più di 1000 dipendenti ha registrato un aumento negli attacchi di phishing rispetto agli anni precedenti.

Ogni professionista IT e della sicurezza chiaramente vorrebbe evitare che la propria organizzazione rientri in queste statistiche. In particolare, vorrebbero:

- **Bloccare malware e phishing,** che cambiano costantemente tecniche per eludere il rilevamento.
- **Interrompere la perdita di dati in generale,** sia tramite dispositivi infetti che con interazioni tra utenti.
- **Ottenere una maggiore visibilità sulla navigazione in Internet dei dipendenti,** al fine di comprendere il panorama specifico delle minacce alla loro organizzazione e rispondere più rapidamente alle violazioni che si verificano.

Questi casi d'uso sono elementi importanti della **sicurezza Zero Trust**, in cui le proprietà Internet e il codice non devono essere implicitamente attendibili e devono quindi essere elaborati in modo sicuro al momento dell'interazione dell'utente.

Per raggiungere questi obiettivi, alcune organizzazioni stanno ricorrendo all'isolamento del browser, in cui la navigazione in Internet dei dipendenti è tenuta separata dalle reti e dall'infrastruttura locali. Implementato in modo completo ed efficiente, l'isolamento del browser è potenzialmente il modo più efficace per mitigare gli attacchi provenienti da Internet. Sfortunatamente, finora è rimasta una tecnologia di nicchia a causa di una serie di problemi, tra cui **costi elevati, esperienze di navigazione scadenti, difficoltà di gestione logistica** e **falle nella sicurezza.**

In questo documento questi problemi sono descritti dettagliatamente al fine di aiutare i team di sicurezza e IT a comprendere meglio le loro esigenze di sicurezza per la navigazione in Internet. È riportato anche un metodo di risoluzione e, infine, viene spiegato come Cloudflare ha integrato tale metodo nella sua rete globale.

Problemi delle strategie comuni di isolamento del browser

Malware, phishing e perdita di dati interessano le organizzazioni in ogni campo e settore. L'isolamento del browser viene comunemente implementato come soluzione per i primi due tipi di minacce, potenziando il blocklist, la corrispondenza di file e gli approcci comportamentali utilizzati da gateway Web sicuri.

In pratica, però, l'isolamento del browser spesso non raggiunge questo obiettivo.

Perché è questo il caso? Consideriamo le limitazioni dei metodi di isolamento del browser più comuni:

Cattura della schermata in streaming dell'attività di navigazione dal cloud

Questo approccio, a volte chiamato "pixel-push", cattura gli eventi nel browser dell'utente finale e li trasmette a un browser remoto ospitato nel cloud che esegue effettivamente le azioni di navigazione e trasmette una sequenza di immagini pixel della finestra del browser remoto all'utente finale. In questo modo, qualsiasi codice dannoso, scaricato automaticamente o tramite un'azione deliberata di un utente, viene tenuto separato dal dispositivo dell'utente finale. E potenziali siti di phishing, come ad esempio le pagine con campi di modulo nome utente/password, possono essere visualizzati in modalità di sola lettura o con un messaggio di avviso aggiunto.

Questo approccio consente di isolare i dispositivi endpoint dal malware e dal phishing. Tuttavia, presenta problemi come:

Latenza dell'utente finale: quando l'isolamento del browser remoto è ospitato nel cloud pubblico o su una rete privata geograficamente limitata, gli utenti finali potrebbero riscontrare una latenza quando sono fisicamente distanti dai datacenter di isolamento del browser. Questo problema si aggrava quando il traffico degli utenti finali passa attraverso altri strumenti di sicurezza, come un gateway Web sicuro, che non sono ospitati negli stessi data center o che richiedono più "passaggi" attraverso container progettati in modo inefficiente.

Costi elevati: la codifica continua di flussi video di pagine Web remote sui dispositivi endpoint dell'utente finale è molto costosa dal punto di vista computazionale. Richiede anche una larghezza di banda significativa, anche se altamente ottimizzata. Questi costi vengono in genere trasferiti ai clienti.

Falle nella sicurezza: poiché il "pixel-push" spesso causa esperienze scadenti per gli utenti finali, molte organizzazioni richiedono il suo utilizzo solo in team con accesso a dati particolarmente sensibili, come quelli relativi a finanza, risorse umane o dirigenti aziendali. L'organizzazione può anche applicare la navigazione remota solo a una piccola percentuale di pagine Web considerate particolarmente rischiose. In ogni caso, l'organizzazione rimarrà esposta, sia tramite dipendenti non protetti che tramite siti considerati affidabili ma che invece sono stati compromessi.

Elevata larghezza di banda necessaria: lo streaming di immagini utilizza molta larghezza di banda, il che può sovraccaricare l'infrastruttura di rete e avere un impatto negativo sull'esperienza dell'utente finale. Inoltre, la densità dei pixel aumenta in modo esponenziale con la risoluzione, il che significa che le sessioni del browser remoto (in particolare i caratteri) sui dispositivi HiDPI possono apparire sfocate.

Scomposizione dei siti Web nel cloud e rimozione di codice dannoso

Questo metodo viene spesso definito manipolazione DOM. Nello sviluppo frontend, DOM, o Document Object Model, è la rappresentazione dei dati degli oggetti che compongono la struttura e il contenuto di una pagina Web. Nella manipolazione DOM, un browser remoto ospitato nel cloud esamina HTML, CSS e altri elementi di una pagina Web e tenta di eliminare codice attivo come Javascript, exploit noti e altri contenuti potenzialmente dannosi. Il browser remoto inoltra quindi questo codice al browser dell'utente finale, che lo utilizza per ricostruire una versione "pulita" della pagina. Inoltre, come per il "pixel-push", la manipolazione DOM può anche contrassegnare determinate pagine come a rischio di phishing.

Poiché la manipolazione DOM trasferisce solo il codice del sito Web e non un flusso completo dell'esperienza di navigazione, richiede una minore larghezza di banda e può portare a esperienze più rapide per gli utenti finali.

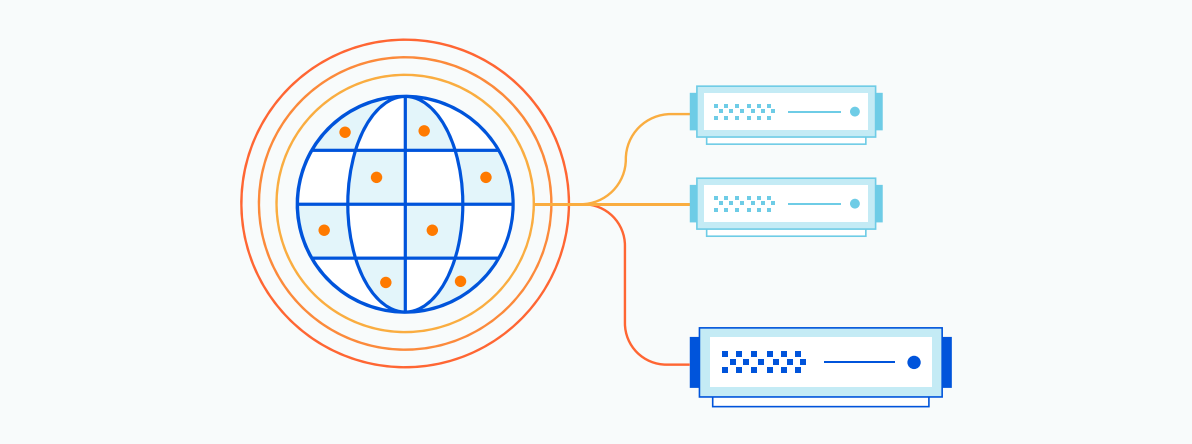
Tuttavia, presenta problemi come:

Latenza dell'utente finale: come con il "pixel-push", se l'isolamento del browser con manipolazione DOM funziona nel cloud pubblico, o su una rete privata geograficamente limitata, gli utenti finali possono ancora riscontrare una latenza quando i server di origine sono troppo lontani o quando l'isolamento del browser e altri strumenti di sicurezza sono ospitati in diversi datacenter.

Interruzione delle esperienze del sito Web: il tentativo di rimozione di codice attivo dannoso, oltre alla ricostruzione di HTML e CSS e di architetture di siti non comuni, inevitabilmente si traduce in pagine danneggiate che non vengono visualizzate correttamente o non vengono visualizzate affatto. Inoltre, i siti Web che funzionano oggi potrebbero non funzionare domani, poiché gli editor potrebbero apportare modifiche quotidiane che interrompono la funzionalità di ricostruzione DOM. La manipolazione DOM fatica persino a supportare servizi comuni a livello aziendale come Google G Suite o Microsoft Office 365. Il risultato è una coda infinita di problemi che richiedono risorse IT significative in un gioco della talpa che va all'infinito.

Costi elevati: alcuni servizi di manipolazione DOM sono ospitati in infrastrutture cloud pubbliche di terze parti, con costi aggiuntivi che in genere vengono trasferiti ai clienti. In ogni caso, l'organizzazione rimarrà esposta, sia tramite dipendenti non protetti che tramite siti considerati attendibili ma che invece sono stati compromessi

Falle nella sicurezza: come per il "pixel-push", l'esperienza completamente inaffidabile dell'utente finale della manipolazione DOM spesso significa che le organizzazioni la utilizzano solo sporadicamente. Inoltre, sebbene la manipolazione DOM sia una forma di isolamento del browser, invia comunque codice di terze parti non attendibile ai dispositivi endpoint. Se il servizio non riesce a identificare il codice dannoso, un rischio costante dato il panorama delle minacce in continua evoluzione, i dispositivi endpoint potrebbero comunque cedere.



Isolamento dell'attività di navigazione in una macchina virtuale su dispositivo

Con questo approccio, il software installato su un dispositivo endpoint crea una macchina virtuale che è isolata dal resto del sistema operativo del dispositivo. Tutta l'attività di navigazione si svolge su questa macchina virtuale, quindi qualsiasi malware scaricato non può infettare il resto del dispositivo. Inoltre, come altri approcci, il software può contrassegnare alcune pagine come a rischio di phishing.

Sfortunatamente, tra i problemi di questo approccio vi sono:

Elevate richieste di CPU e RAM: l'esecuzione di una macchina virtuale separata può rallentare molti PC, con conseguenti esperienze di navigazione non soddisfacenti per gli utenti finali.

Difficoltà di gestione degli endpoint: l'isolamento del browser tramite software locale richiede ai team IT di installare e aggiornare il suddetto software su ogni dispositivo endpoint: un compito quasi impossibile per le grandi organizzazioni. Questa complessità logistica peggiora ulteriormente quando le organizzazioni hanno un gran numero di lavoratori in remoto o se impiegano appaltatori di terze parti che non utilizzano dispositivi forniti dall'azienda.

Problemi di compatibilità mobile: l'isolamento del browser basato su una macchina virtuale sul dispositivo richiede implementazioni specifiche del sistema operativo. I dispositivi mobili spesso non sono supportati.

Errori di isolamento: i servizi di isolamento del browser locale riscontrano periodicamente vulnerabilità che consentono al codice dannoso di accedere al sistema operativo principale. In queste circostanze, i team IT o gli utenti finali devono installare manualmente patch e aggiornamenti. Ma se la patch non viene installata correttamente, il dispositivo endpoint potrebbe rimanere vulnerabile.

Esperienza non soddisfacente degli utenti finali: le implementazioni basate su macchine virtuali richiedono spesso agli utenti finali di utilizzare browser, finestre o desktop "virtualizzati" separati. Ciò richiede la dovuta formazione e crea un carico per il supporto IT.

Questi problemi iniziali ne creano di altri

Le conseguenze immediate come costi elevati, esperienze negative per gli utenti finali e difficoltà di gestione degli endpoint non sono gli unici problemi degli approcci comuni all'isolamento del browser.

Un altro problema è dato dalle conseguenze a lungo termine della compromissione del dispositivo. Quando gli utenti finali accedono ad applicazioni sensibili tramite un dispositivo compromesso, il malware può accedere ai dati dell'applicazione senza che l'utente se ne accorga.

Inoltre, tutti questi approcci all'isolamento del browser hanno difficoltà a prevenire determinati tipi di perdita di dati. I soggetti interni possono ancora essere in grado di caricare e inviare informazioni sensibili tramite e-mail o di inserirle in moduli online.

Un approccio migliore all'isolamento del browser in remoto

Le organizzazioni vogliono comunque adottare la navigazione remota nonostante i problemi menzionati nella sezione precedente.

Fortunatamente, alcune tecnologie possono aiutare:

Problema	Soluzione
Latenza	**Uso di una rete perimetrali di grandi dimensioni:** anziché ospitare l'isolamento del browser in un numero limitato di datacenter di cloud pubblici, fallo su una rete perimetrale globale vicina agli utenti finali. Inoltre, utilizza un software di isolamento del browser che risiede negli stessi datacenter dei gateway Web protetti e di altri strumenti di sicurezza.
Requisiti di larghezza di banda elevata	**Nessun "pixel-push":** lo streaming di immagini dell'attività del browser remoto non è pratico da implementare per le imprese più grandi, sia dal punto di vista dei costi che dell'esperienza utente.
Interruzione delle esperienze del sito Web	**Uso della tecnologia browser nativa:** i browser remoti che utilizzano la tecnologia già integrata nelle app di navigazione dei dispositivi endpoint comuni sono più affidabili nel ricostruire accuratamente tutti i tipi di siti.
Costi di elaborazione elevati	**Cloud computing di nuova generazione:** evita l'isolamento del browser remoto ospitato nel cloud pubblico. E utilizza tecniche di elaborazione serverless efficienti che migliorano la virtualizzazione e la containerizzazione eliminando l'orchestrazione e la gestione delle risorse del server sottostanti, al fine di utilizzare tali risorse in modo più efficace.
Falle nella sicurezza	**Uso della tecnologia nativa del browser:** piuttosto che cercare di decidere quale codice inviare o bloccare, la tecnologia di navigazione nativa può evitare del tutto l'invio. Piuttosto, è in grado di inviare solo l'ultimo passaggio del processo di rendering che disegna la pagina.
Difficoltà specifiche dell'endpoint	**Nessun isolamento del browser locale:** l'isolamento dell'attività di navigazione sui dispositivi endpoint è troppo lento e difficile da gestire e ciò rende l'approccio già superato.

Per capire come funzionano in pratica queste tecnologie, considera l'esempio di Cloudflare Browser Isolation, che è integrato con la nostra piattaforma Zero Trust.

Cloudflare rende la navigazione remota più conveniente e da meno problemi all'utente finale

A un livello elevato, Cloudflare evita le difficoltà specifiche degli endpoint semplicemente utilizzando una rete perimetrale globale anziché dispositivi endpoint. Più specificamente, la tecnologia Cloudflare evita anche gli altri problemi:

Problema	Soluzione	Implementazione Cloudflare
Latenza	Uso di una rete perimetrale di grandi dimensioni	L'isolamento del browser remoto avviene in ogni datacenter nella rete perimetrale di Cloudflare, che si estende su oltre 200 città in 100 paesi e si trova entro 100 millisecondi dal 95% della popolazione mondiale connessa a Internet. Questa stessa infrastruttura offre servizi DNS e CDN globali a latenza ultra-bassa. Inoltre, la nostra navigazione remota interagisce perfettamente con il nostro proxy di inoltro per applicare tutti gli altri filtri (come il blocco di una parte della pagina) e le ispezioni senza richiedere più passaggi e saltare tra diverse soluzioni puntuali.
Requisiti di larghezza di banda elevata	Tecnologia nativa per browser	La tecnologia Network Vector Rendering di Cloudflare (scopri di più di seguito) trasmette i comandi di disegno anziché le immagini in pixel o il codice con "scrubbing". Questo metodo richiede una parte della larghezza di banda consumata dalla normale navigazione o dalla manipolazione DOM, per non parlare del "pixel-push".
Interruzione Sito web del sito Web	Tecnologia nativa per browser	Il browser remoto di Cloudflare si basa sul motore open-source Chromium, su cui sono costruiti Google Chrome e ventuno altri browser. Un investimento costante nel motore Chromium garantisce i più elevati livelli di compatibilità del sito Web. Inoltre, poiché la tecnologia Network Vector Rendering di Cloudflare trasmette i comandi di disegno anziché il codice "pulito", garantisce che anche le pagine Web più complesse non vengano interrotte.
Costi di elaborazione elevati	Cloud computing di nuova generazione	Poiché l'isolamento del browser Cloudflare opera sulla nostra rete, non dobbiamo rifarci dei costi del cloud pubblico sui clienti. E poiché siamo in grado di orchestrare e gestire le risorse del server in modo molto efficiente, evitiamo gli avviamenti a freddo di pochi secondi che spesso interessano le applicazioni ospitate sul cloud pubblico.
Falle nella sicurezza	Tecnologia nativa per browser	Trasmettendo comandi di disegno vettoriale leggero piuttosto che qualsiasi codice originale del sito Web, Cloudflare elimina il rischio di esecuzione di codice non attendibile sul dispositivo endpoint. Il malware non rilevato compromette solo il browser remoto senza influire sull'endpoint. E dal momento che Cloudflare offre esperienze avanzate per gli utenti finali, le aziende possono applicare la navigazione remota a casi d'uso meno rischiosi che altrimenti potrebbero non essere protetti.
	Granulare controllo del comportamento dell'utente finale	Gli strumenti di prevenzione della perdita di dati in genere proteggono i dati mentre sono in transito sulla rete, consentendone o bloccandone la trasmissione. Cloudflare Browser Isolation fornirà agli amministratori un controllo granulare su: • Autorizzazioni copia/incolla/stampa • Operazioni di upload/download • Attività generica della tastiera • Autorizzazioni per l'inserimento nei moduli • Posizione di archiviazione dei file scaricati* *Presto disponibile

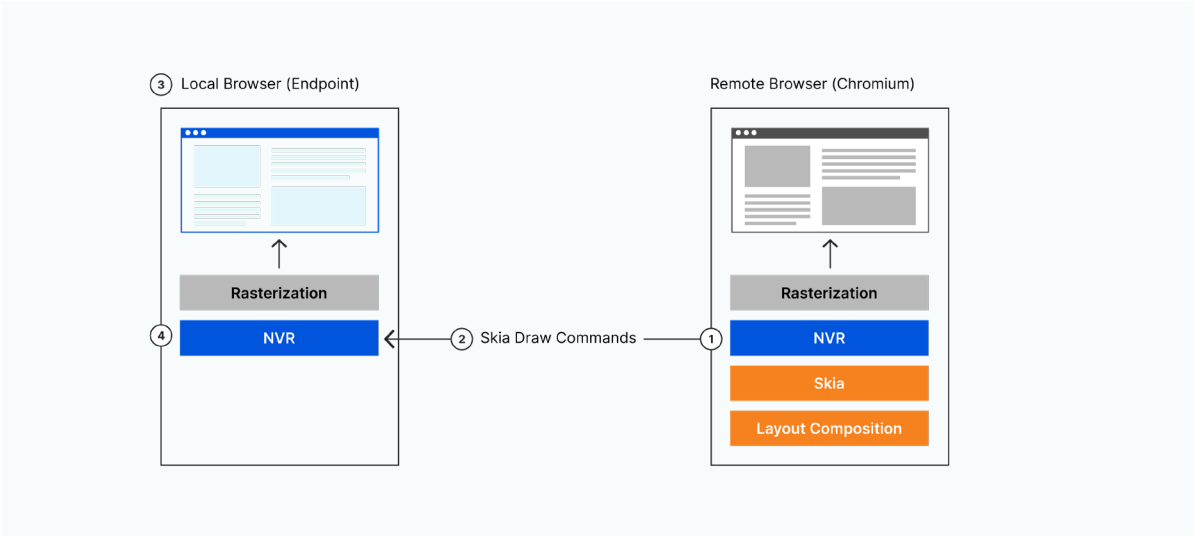
Continua a leggere per maggiori dettagli sulla tecnica NVR descritta sopra:

Network Vector Rendering offre migliori esperienze per gli utenti finali e colma le falle nella sicurezza

Come accennato in precedenza, il browser remoto di Cloudflare si basa su Chromium. Una caratteristica architettonica chiave del browser Chromium è il suo utilizzo di Skia, un motore di grafica multipiattaforma ampiamente utilizzato per Android, Google Chrome, Chrome OS, Mozilla Firefox e molti altri browser. Tutti i briwser compatibili con HTML5 possono eseguire il rendering di Skia. Tutto ciò che è visibile in una finestra del browser Chromium viene reso tramite il livello di rendering di Skia. Ciò include l'interfaccia utente delle finestre dell'applicazione, come i menu, ma ancora più importante, l'intero contenuto della finestra della pagina Web viene visualizzato tramite Skia. Cloudflare può persino isolare i file scaricati e spostarli in varie posizioni in base alle esigenze dell'utente finale.

La tecnologia Network Vector Rendering (NVR) di Cloudflare intercetta i comandi di disegno Skia del browser Chromium remoto, li tokenizza e li comprime, quindi li crittografa e li trasmette attraverso il cavo a qualsiasi browser Web compatibile con HTML5 in esecuzione localmente sul desktop dell'endpoint o sul dispositivo mobile. I comandi dell'API Skia acquisiti da NVR sono pre-rasterizzati, il che significa che sono estremamente compatti e poiché Skia è così diffuso, la navigazione remota di Cloudflare funziona su qualsiasi browser Web moderno.

Network Vector Rendering è anche più sicuro. Come accennato in precedenza, poiché Cloudflare fornisce ai dispositivi endpoint i comandi di disegno e non il codice effettivo del sito Web, il trasporto di dati non è un vettore di attacco.



Scopri di più e inizia subito

Dal giorno in cui Cloudflare è nato, la nostra missione è stata quella di aiutare a costruire un Internet migliore e democratizzare le tecnologie che in precedenza erano accessibili solo a grandi aziende con reti sofisticate, team IT dedicati e budget enormi. Il miglioramento dell'isolamento del browser remoto è una parte importante di questa missione.

Rendendo l'isolamento del browser più conveniente e fornendo esperienze eccezionali agli utenti finali, speriamo di raggiungere sempre più organizzazioni. Come in un passato non troppo lontano in cui la crittografia HTTPS era riservata alle pagine di accesso "sensibili" e ai checkout di e-commerce, crediamo che fidarsi del codice arbitrario di un sito Web sembrerà arcaico quanto creare il nuovo paradigma di navigazione Zero Trust.

Per maggiori informazioni su Cloudflare Browser Isolation e su come può aiutarti a ottenere la navigazione Zero Trust, visita il sito all'indirizzo https://www.cloudflare.com/products/zero-trust/browser-isolation/