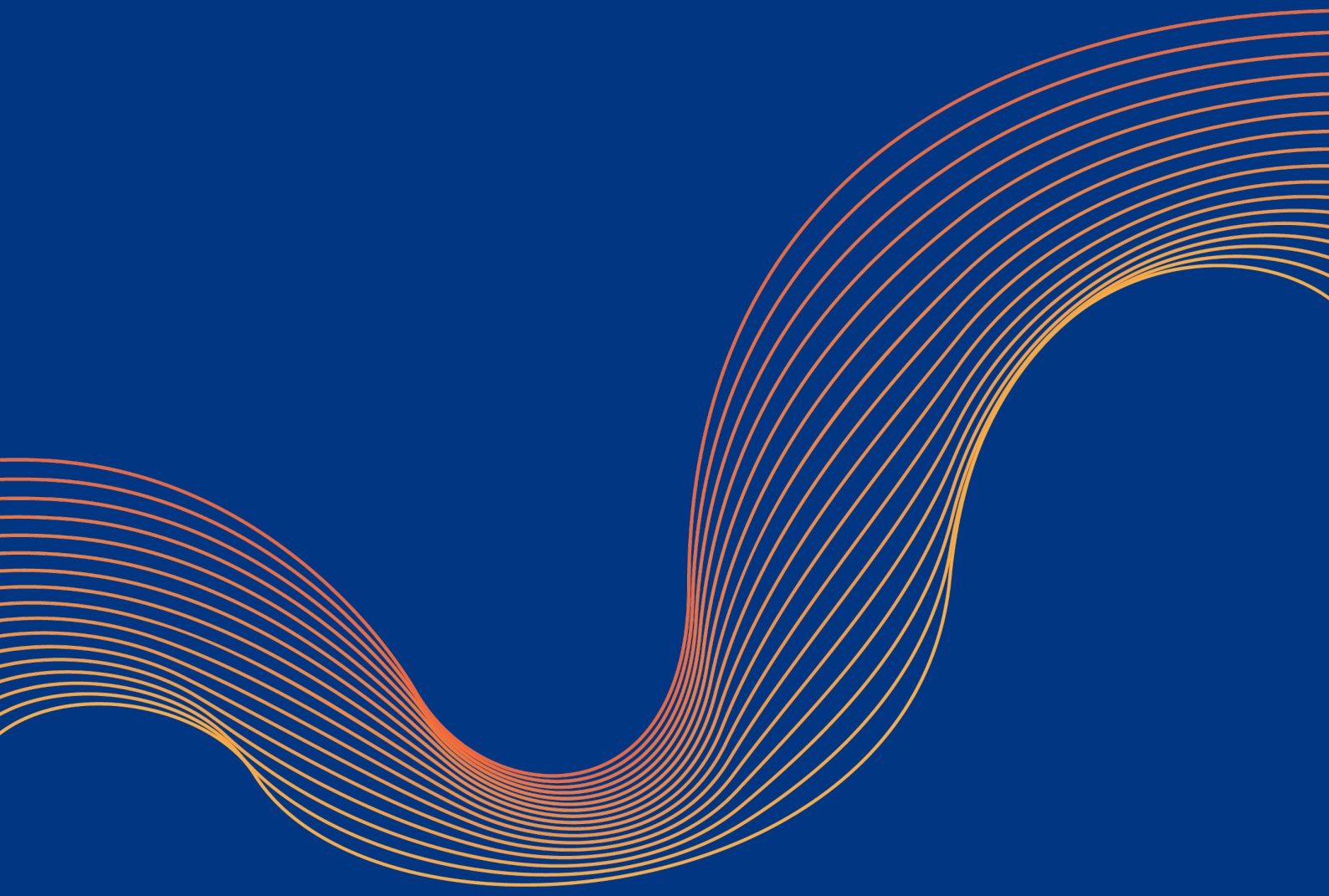
CLOUDFLARE

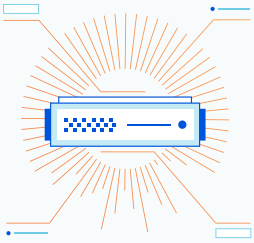
일반적인 브라우저 격리 문제와 이를 극복하는 방법

인터넷 브라우징과 Zero Trust 보안의 만남



+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

색인



소개

IT와 보안팀이 공용 인터넷을 믿지 않는 데는 이유가 있습니다. 2020년에 일어난 데이터 유출 사건의 39%가 피싱과 맬웨어에 의해 이루어졌다고 한 Verizon 보고서에서 보고했습니다. 또한, Cloudflare가 의뢰한 Forrester Consulting의 연구에 따르면 2020년에 직원 수 1,000명 이상의 기업 중 61%에서 그 전 해와 비교했을 때 피싱 공격 수가 증가했다고 합니다.

모든 IT 및 보안 전문가는 자신의 조직이 이러한 통계에 포함되는 것을 막으려고 합니다. 구체적으로, 이들은 다음과 같은 노력을 하려고 합니다.

- **맬웨어와 피싱을 차단합니다.** 이들은 감지되는 것을 막기 위해 전략을 지속적으로 바꿉니다.
- **전반적인 데이터 손실을 막습니다.** 데이터 손실은 감염된 장치를 통해 또는 사용자 간의 상호작용으로 인해 발생할 수 있습니다.
- **직원의 인터넷 브라우징에 대한 더 나은 가시성을 얻습니다.** 이는 자신이 속한 조직의 구체적인 위협 환경을 이해하고 발생하는 유출 사건에 더 빠르게 대응하기 위한 것입니다.

이 용례는 **Zero Trust 보안**의 중요한 요소입니다. 다시 말해, 인터넷 자산과 코드를 암묵적으로 신뢰해서는 안 되며, 따라서 사용자와의 상호작용 시에 안전하게 처리해야 하는 경우입니다.

이러한 목표를 달성하기 위해서 일부 조직에서는 직원의 인터넷 검색이 로컬 네트워크와 인프라와는 분리되는 브라우저 격리로 눈을 돌리고 있습니다. 브라우저 격리는 철저하고 효율적으로 도입할 경우 인터넷에서 발생하는 공격을 완화하는 가장 강력한 방법이 됩니다. 하지만, 안타깝게도 이 방법은 여러 문제, 예를 들어 **많은 비용, 좋지 못한 브라우징 경험, 물류 관리의 어려움,** 그리고 **보안상의 구멍 등의 이유로 지금까지는 주류가 아닌 기술이었습니다.**

이 백서에서는 보안 팀과 IT 팀이 자체의 인터넷 브라우징 보안 요구사항을 더 잘 이해할 수 있도록 이러한 어려움을 자세히 설명합니다. 또한, 이러한 어려움을 극복하기 위한 방법을 이야기하며, 마지막으로 Cloudflare에서 어떻게 이 방법을 자사의 전역 네트워크에 통합했는지 설명합니다.

일반적인 브라우저 격리 전략의 난점

맬웨어, 피싱, 데이터 손실은 모든 산업과 업계의 조직에 영향을 줍니다. 이 중 첫 두 위협 유형에 대한 솔루션으로는 브라우저 격리가 가장 많이 배포되며, 보안 웹 게이트웨이에서 사용하는 차단 목록, 파일 매칭, 행동적 접근 방식을 강화합니다.

하지만 현실에서는 브라우저 격리로 이러한 목표를 달성하지 못하는 경우가 많습니다.

그 이유는 무엇일까요? 가장 흔하게 사용되는 브라우저 격리 방법의 한계를 생각해 봅시다.

클라우드 검색 활동의 스크린 캡처를 스트리밍

때로는 '픽셀 푸싱'이라고 불리기도 하는 이 접근 방식에서는 최종 사용자 브라우저 내의 이벤트를 캡처하여 클라우드에 호스팅된 원격 브라우저로 전송합니다. 원격 브라우저는 실제 브라우징 동작을 수행해 원격 브라우저 윈도우의 일련의 픽셀 이미지를 최종 사용자의 윈도우로 전송합니다. 이러한 방식을 사용하면 모든 악성 코드는 자동으로 다운로드되든, 아니면 사용자의 의도적인 행동으로 인해 다운로드되든 관계 없이 최종 사용자의 장치와는 분리되어 있게 됩니다. 또한, 사용자명/패스워드 양식 필드가 있는 페이지와 같은 잠재적인 피싱 사이트는 읽기 전용으로 표시되거나 경고 메시지가 추가되어 표시될 수도 있습니다.

이러한 접근 방식으로 엔드포인트 장치를 맬웨어와 피싱으로부터 잘 격리할 수 있습니다. 하지만, 다음과 같은 문제점이 존재합니다.

최종 사용자 지연: 원격 브라우저 격리가 공용 클라우드 또는 지리적으로 제한된 사설 네트워크에 호스팅되는 경우, 최종 사용자는 브라우저 격리 데이터 센터로부터 물리적으로 멀리 떨어져 있다면 지연을 경험할 수 있습니다. 이 문제는 최종 사용자의 트래픽이 동일한 데이터 센터에 호스팅되지 않거나 비효율적으로 구성되어 있는 컨테이너를 여러 차례 '통과'해야 하는 보안 웹 게이트웨이와 같은 다른 보안 도구를 거칠 때 더 심해집니다.

많은 비용: 원격 웹페이지의 동영상 스트리밍을 최종 사용자의 엔드포인트 장치로 지속해서 암호화하는 것은 비용이 아주 많이 듭니다. 또한, 최적화가 아주 잘 된 경우에도 대역폭이 많이 필요합니다. 이러한 비용은 대체로 소비자에게 전가됩니다.

보안 간극: '픽셀 푸싱'은 주로 최종 사용자 경험 악화로 이어지기 때문에 많은 조직에서는 이 기능을 회계 팀, 인사 팀, 회사 중역 등 특히 중요한 데이터에 접근할 수 있는 팀의 경우에만 사용합니다. 이러한 조직에서는 또한 원격 브라우징을 특히 위험성이 높다고 간주되는 극히 일부의 웹 페이지에만 적용할 수도 있습니다. 어느 경우이든, 조직은 보호되지 않은 직원 또는 손상된 '믿을 수 있는 사이트'를 통한 피해에 계속 노출되어 있게 됩니다.

높은 대역폭 요구사항: 이미지 스트리밍에는 넓은 대역폭이 필요하므로 네트워크 인프라에 과도한 부담을 주고 최종 사용자 경험에 부정적인 영향을 줄 수 있습니다. 여기에 더하여 픽셀 밀도가 해상도에 따라 기하급수적으로 증가하므로 고DPI 장치에서는 원격 브라우저 세션(특히 폰트)이 흐리거나 초점이 안 맞는 것처럼 보일 수 있습니다.

클라우드 상에서 웹 사이트를 분석해 악성 코드 제거하기

이 방법은 흔히 DOM 조작이라고 불립니다. 프런트엔드 개발에서 문서 개체 모델(DOM)은 웹페이지의 구조와 콘텐츠를 구성하는 개체를 데이터로 표현한 것입니다. DOM 조작에서는 클라우드로 호스팅된 원격 브라우저가 웹페이지의 HTML, CSS, 기타 요소를 검사해 Javascript, 알려진 취약성, 기타 잠재적으로 악의적일 수 있는 콘텐츠 등 활성 상태의 코드를 제거하려고 시도합니다. 그런 다음, 원격 브라우저가 이 코드를 최종 사용자의 브라우저로 전송하며, 이는 페이지의 '깨끗한' 버전을 재구성하는 데에 사용됩니다. 여기에 더해 "픽셀 푸싱"의 경우와 마찬가지로 DOM 조작을 통해 특정 페이지를 피싱 위협으로 표시할 수 있습니다.

DOM 조작은 브라우징 경험 전체를 스트리밍하는 것이 아니라 웹 사이트 코드만을 전송하기 때문에 대역폭이 덜 필요하고 더 빠른 최종 사용자 경험을 제공할 수 있습니다.

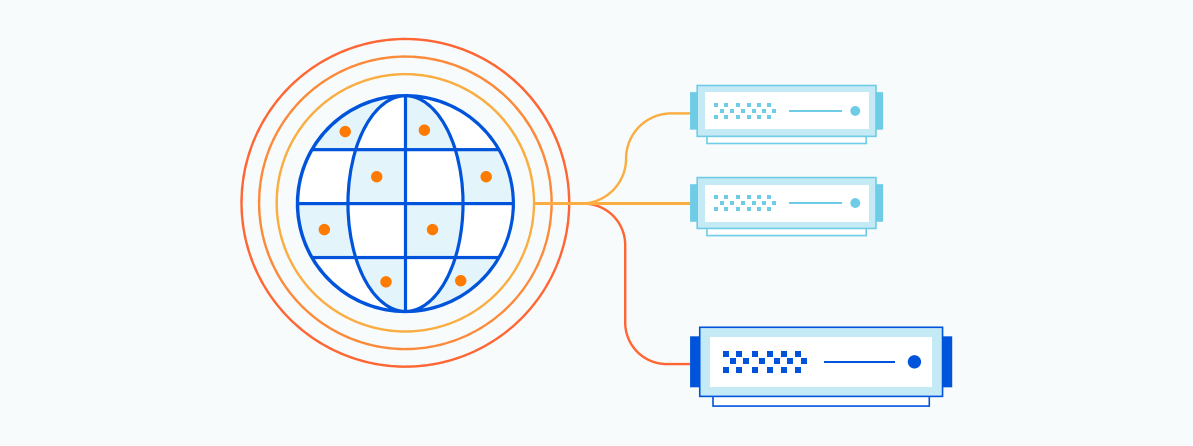
하지만, 다음과 같은 문제점이 존재합니다.

최종 사용자 지연: '픽셀 푸싱'과 마찬가지로 DOM 조작 브라우저 격리가 공용 클라우드 또는 지리적으로 제한된 사설 네트워크에 호스팅되는 경우, 최종 사용자는 여전히 원본 서버가 너무 멀리 떨어져 있거나 브라우저 격리와 기타 보안 도구가 서로 다른 데이터 센터에 호스팅된 경우에는 지연을 경험할 수 있습니다.

웹 사이트 깨짐을 경험: 악의적인 활성 코드를 제거하고, HTML과 CSS를 재구성하며, 흔하지 않은 사이트 구조를 재구성하는 것은 필연적으로 올바르게 렌더링되지 않거나 아예 렌더링되지 않는 깨진 페이지로 이어지게 됩니다. 여기에 더해 사이트 제공자가 DOM 재구성 기능을 작동하지 못하게 하는 변화를 발생시킬 수 있기 때문에 오늘은 작동했던 웹 사이트가 내일은 작동하지 못할 수도 있습니다. DOM 조작 기법은 Google G Suite나 Microsoft Office 365와 같은 여러 기업에서 흔히 사용되는 서비스조차도 잘 지원하지 못합니다. 따라서 상당한 양의 IT 리소스를 요구하는 문제가 마치 끝없는 두더지 잡기 게임처럼 무한히 이어지는 사태가 벌어지게 됩니다.

많은 비용: 일부 DOM 조작 서비스는 서드파티 공용 클라우드 인프라에 호스팅되어 추가 비용이 발생하며 이는 대체로 고객에게 전가됩니다. 어느 경우건 조직은 보호되지 않은 직원 또는 손상된 '믿을 수 있는 사이트'를 통한 피해에 계속 노출되어 있게 됩니다

보안 간극: '픽셀 푸싱'과 마찬가지로 DOM 조작의 신뢰성이 없는 최종 사용자 경험 때문에 조직에서는 오직 이 기법을 산발적으로 사용하게 됩니다. 또한, DOM 조작 기법은 브라우저 격리 기법 중 하나이기는 하지만 여전히 믿을 수 없는 서드파티 코드를 엔드포인트 장치로 전송하는 기법입니다. 계속해서 발생하는 위협 환경에서는 지속적인 위험이 되는 서비스가 악성 코드 식별에 실패하는 경우 엔드포인트 장치가 여전히 공격을 받을 수 있습니다.



장치상의 가상 머신에서 브라우징 활동 격리하기

이 접근 방식에서는 엔드포인트 장치에 설치된 소프트웨어가 장치의 나머지 운영체제와는 격리된 가상 머신을 생성합니다. 모든 브라우징 활동은 이 가상 머신에서 일어나기 때문에 다운로드된 모든 맬웨어는 장치의 나머지 부분을 감염시킬 수 없습니다. 여기에 더해, 다른 접근 방식과 마찬가지로 소프트웨어가 특정 페이지를 피싱 위협으로 표시할 수 있습니다.

하지만, 이러한 접근 방식에는 다음과 같은 문제가 있습니다.

- **높은 CPU 및 RAM 요구사항:** 별도의 가상 머신을 구동하면 많은 PC가 느려져서 최종 사용자가 느린 브라우징을 경험하게 될 수 있습니다.
- **엔드포인트 관리의 어려움:** 로컬 소프트웨어를 통하여 브라우저를 격리하려면 IT 팀이 모든 엔드포인트 장치에 이 소프트웨어를 설치하고 업데이트해야 합니다. 이는 큰 조직의 경우 꽤 어려운 일입니다. 이 물류적인 복잡성은 조직에 원격 근무자가 많거나 회사가 발행한 장치를 사용하지 않는 서드파티 계약자를 운용하는 경우 더 심해집니다.
- **모바일 호환성 문제:** 장치상의 가상 머신을 기반으로 하는 브라우저 격리 방법은 운영체제별로 다른 도입 방법을 필요로 합니다. 모바일 장치는 대개 지원되지 않습니다.
- **격리 실패:** 로컬 브라우저 격리 서비스는 주기적으로 악성 코드가 주 운영체제에 접근할 수 있는 취약성이 생깁니다. 이러한 경우에는 IT 팀 또는 최종 사용자가 수동으로 패치하고 업데이트를 설치해야 합니다. 하지만, 패치가 올바르게 설치되지 않은 경우, 엔드포인트 장치가 취약한 채로 유지될 수 있습니다.
- **최종 사용자 경험 악화:** 가상 머신 기반 기법을 도입하는 경우 대개 최종 사용자가 "가상화된" 별도의 브라우저, 윈도우, 데스크탑을 사용해야 합니다. 이를 위해서는 교육이 필요하며, IT 지원상의 부담이 발생합니다.

이러한 즉각적인 문제점 때문에 추가적인 문제가 생깁니다

많은 비용, 최종 사용자 경험 악화, 엔드포인트 관리의 어려움등 즉각적인 문제점만이 주로 사용되는 브라우저 격리 방법의 유일한 난점인 것은 아닙니다.

또다른 문제점으로는 장치 손상의 장기적인 영향이 있습니다. 최종 사용자가 중요한 애플리케이션에 손상된 장치를 사용해 로그인하는 경우, 맬웨어가 해당 애플리케이션의 데이터에 사용자가 모르는 사이에 접근할 수 있습니다.

여기에 더해 이 모든 브라우저 격리 접근법은 특정 유형의 데이터 손실을 잘 방지하지 못합니다. 내부자는 여전히 이메일을 통해 중요한 정보를 업로드하고 전송하거나 온라인 서식에 입력할 수 있습니다.

원격 브라우저 격리를 위한 더 나은 접근법

이전 섹션에서 언급한 문제가 존재함에도 불구하고 여러 조직에서는 원격 브라우징을 도입하려고 합니다.

다행히도, 다음과 같은 특정한 기술이 도움이 됩니다.

문제	솔루션
대기 시간	**대형 에지 네트워크 사용:** 브라우저 격리를 제한된 수의 공용 클라우드 데이터 센터에 호스팅하는 대신 동일한 서비스를 최종 사용자가 어디에 있건 그 근처에 위치해 있는 전역 에지 네트워크에 호스팅합니다. 여기에 더해 보안 웹 게이트웨이와 기타 보안 도구와 동일한 데이터 센터에 설치된 브라우저 격리 소프트웨어를 사용합니다.
높은 대역폭 요건	**픽셀 푸싱 없음:** 원격 브라우저 활동의 이미지를 스트리밍하는 것은 대형 기업의 경우 비용 및 사용자 경험이라는 측면 모두에서 실용적이지 않습니다.
웹 사이트 깨짐 경험	**네이티브 브라우저 기술 사용:** 대부분의 엔드포인트 장치의 브라우징 앱에 이미 내장되어 있는 기술을 사용하는 원격 브라우저는 다양한 사이트를 더 신뢰성 있게 정확히 재현할 수 있습니다.
높은 컴퓨팅 비용	**차세대 클라우드 컴퓨팅:** 공용 클라우드에 호스팅된 원격 브라우저 격리를 피하고, 기반이 되는 서버 리소스의 조정 및 관리의 필요성을 없애서 리소스를 더 효율적으로 사용하게 하여 가상화와 컨테이너화를 개선하는 효율적인 서버리스 컴퓨팅 기법을 사용합니다.
보안 간극	**네이티브 브라우저 기술 사용:** 네이티브 브라우저 기술은 어떤 코드를 전송하고 차단할 지 판별하려고 시도하는 대신 코드를 전송하는 것 자체를 피하고 페이지를 표시하는 렌더링 과정의 마지막 단계만을 전송하게 만들 수 있습니다.
엔드포인트별 문제	**로컬 브라우저 격리 없음:** 엔드포인트 장치에서 브라우징 활동을 격리하는 것은 느리고 관리하기 어려우므로 이 접근법은 완전히 구시대의 접근 방식이 됩니다.

이러한 기술이 실제로 어떻게 작동하는지 알아보기 위하여 Cloudflare의 Zero Trust 플랫폼에 태생적으로 통합되어 있는 Cloudflare 브라우저 격리를 알아보겠습니다.

Cloudflare가 원격 브라우징을 비용효율적이며 최종 사용자에게 장애를 덜 일으키게 만드는 방법

높은 수준에서 Cloudflare는 단순히 엔드포인트 장치가 아닌 전역 에지 네트워크에서 구동해 엔드포인트별 문제를 피합니다. 더 자세히 말하자면, Cloudflare의 기술은 다른 문제들 또한 해소합니다.

문제	솔루션	Cloudflare 구현
 대기 시간	대형 에지 네트워크의 사용	원격 브라우저 격리는 전 세계 100개 국가의 200개 도시에 걸쳐 있어 인터넷 연결 인구의 95%와 100ms 이내에서 작동하는 Cloudflare 에지 네트워크의 모든 데이터 센터에서 실행됩니다. 바로 이 인프라로 초저레이턴시 전역 DNS 및 CDN 서비스를 제공합니다. 여기에 더해 Cloudflare의 원격 브라우징은 전방 프록시와 깔끔하게 상호작용하므로 여러 번의 패스와 서로 다른 포인트 솔루션 사이를 왔다갔다 할 필요 없이 모든 다른 필터(예를 들어, 페이지 일부를 차단하는 등) 및 검사를 도입할 수 있습니다.
 높은 대역폭 요건	네이티브 브라우저 기술	Cloudflare의 네트워크 벡터 렌더링 기술(아래에서 더 알아보기)은 픽셀 이미지나 "정제된" 코드 대신 그리기 명령을 전송합니다. 이 기법은 일반적인 브라우징이나 DOM 조작('픽셀 푸싱'은 논외)에 사용되는 대역폭의 일부만을 필요로 합니다.
 웹 사이트 깨짐 경험	네이티브 브라우저 기술	Cloudflare의 원격 브라우저는 Google Chrome과 21개의 다른 흔한 브라우저가 구축되어 있는 오픈소스 Chromium 엔진을 기반으로 합니다. Chromium 엔진에는 지속해서 대규모 투자가 진행 중이므로 최고 수준의 웹 사이트 호환성이 보장됩니다. 또한, Cloudflare의 네트워크 벡터 렌더링 기술은 "정제된" 코드 대신 그리기 명령을 전송하기 때문에 가장 복잡한 웹 페이지도 깨지지 않습니다.
 높은 컴퓨팅 비용	차세대 클라우드 컴퓨팅	Cloudflare 브라우저 격리는 Cloudflare의 네트워크 상에서 운영되기 때문에 고객에게 공용 클라우드 비용을 전가하지 않아도 됩니다. 또한, Cloudflare는 서버 리소스를 효율적으로 구성하고 관리할 수 있기 때문에 공용 클라우드에 호스팅된 애플리케이션에 흔히 영향을 주는, 몇 초간 지속되는 콜드 스타트를 피할 수 있습니다.
 보안 간극	네이티브 브라우저 기술	원본 웹 사이트 코드 대신 가벼운 벡터 그리기 명령을 전송해 Cloudflare는 신뢰할 수 없는 코드가 엔드포인트 장치에서 실행되는 위험을 제거해 줍니다. 감지되지 못한 맬웨어는 엔드포인트에 영향을 주지 않고 원격 브라우저만을 손상시킵니다. 또한, Cloudflare는 강력한 최종 사용자 경험을 제공하기 때문에 회사에서는 사용하지 않을 경우 보호되지 않을 덜 위험한 사용 사례에도 원격 브라우징을 도입할 수 있습니다.
	최종 사용자 행동의 세밀한 제어	데이터 손실 방지 도구는 일반적으로 데이터가 네트워크상에서 전송 중일 때 전송을 허용하거나 차단하는 방식으로 데이터를 보호합니다. Cloudflare 브라우저 격리를 사용하면 관리자는 다음과 같은 행동을 세부적으로 제어할 수 있습니다. • 복사/붙여넣기/인쇄 권한 • 업로드/다운로드 행동 • 전반적인 키보드 활동 • 서식 입력 권한 • 다운로드된 파일이 저장된 위치* *출시 예정

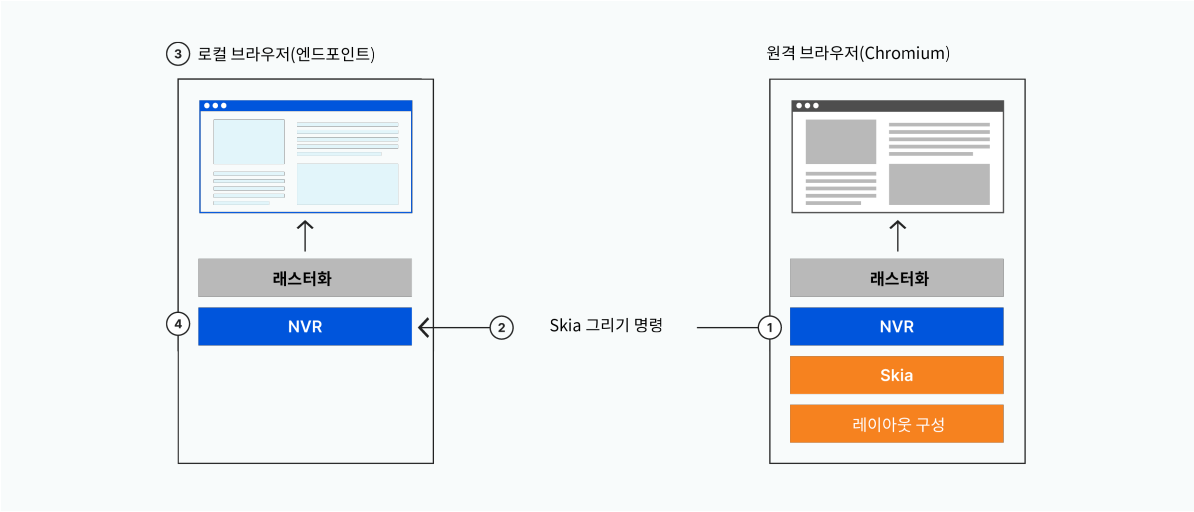
계속 읽으면서 위에 설명된 NVR 기술에 대해 더 알아보십시오.

네트워크 벤더 렌더링으로 더 나은 최종 사용자 경험을 제공하고 보안 간극을 메움

위에서 언급했듯이 Cloudflare의 원격 브라우저는 Chromium을 기반으로 합니다. Chromium 브라우저의 구조적인 주요 기능 중 하나는 안드로이드, Google Chrome, Chrome OS, Mozilla Firefox, 기타 다른 브라우저에서 널리 사용되는 플랫폼 간 그래픽 엔진인 Skia 를 사용한다는 것입니다. 모든 HTML5를 준수하는 브라우저는 Skia를 렌더링할 수 있습니다. Chromium 브라우저 윈도우에 표시되는 모든 것은 Skia 렌더링 계층을 통해 렌더링됩니다. 여기에는 메뉴와 같은 애플리케이션 윈도우 UI가 포함되지만, 가장 중요한 것은 웹페이지 윈도우의 모든 콘텐트가 Skia를 통해 렌더링된다는 점입니다. Cloudflare는 심지어 다운로드된 파일을 격리하고 최종 사용자의 요구사항에 따라 다양한 위치로 이동시킬 수도 있습니다.

Cloudflare의 네트워크 벡터 렌더링(NVR) 기술은 원격 Chromium 브라우저의 Skia 그리기 명령을 가로채고, 토큰화하며, 압축 후 암호화해서 유선으로 엔드포인트 데스크탑 또는 모바일 장치에서 로컬로 가동 중인 HTML5를 준수하는 웹 브라우저로 전송합니다. NVR이 가로채는 Skia API 명령은 래스터화 이전의 명령으로, 고도로 콤팩트합니다. 또한, Skia는 굉장히 많은 곳에서 사용되기 때문에 Cloudflare의 원격 브라우징은 대부분의 현대적인 웹 브라우저에서 작동합니다.

네트워크 벡터 렌더링은 또한 더 안전합니다. 위에서 언급했듯, Cloudflare는 엔드포인트 장치에 실제 웹 사이트 코드가 아닌 그리기 명령을 전달하므로 기반이 되는 전송된 데이터는 공격 벡터가 아닙니다.



자세히 알아보고 시작하세요

Cloudflare는 창립 이래 더 나은 인터넷을 구축하고 정교한 네트워크, 전담 IT 팀, 막대한 예산을 갖춘 대형 회사에서만 접근할 수 있었던 기술을 민주화하도록 지원하는 것을 목표로 해 왔습니다. 더 나은 원격 브라우저 격리는 이 목표의 중요한 일부입니다.

브라우저 격리를 더 비용효율적으로 만들고, 탁월한 최종 사용자 경험을 제공함으로써 Cloudflare는 더 많은 조직에서 이 기술의 진정한 가치를 경험할 수 있기를 바랍니다. HTTPS 암호화 기법이 "중요한" 로그인 페이지와 전자 상거래 체크아웃 전용이었던, 그다지 멀지 않은 과거처럼, 임의의 웹 사이트 코드를 신뢰하는 것이 Zero Trust 브라우징의 새로운 패러다임을 만들어내는 것만큼 오래 전의 일처럼 보이게 될 것으로 믿습니다.

Cloudflare 브라우저 격리 자체와 어떻게 브라우저 격리가 Zero Trust 브라우징을 달성하는 데 도움이 되는지 알아보려면, 다음 웹 사이트를 방문해 주세요
https://www.cloudflare.com/products/zero-trust/browser-isolation/