CLOUDFLARE

제품 요약

Cloudflare 브라우저 격리
인터넷을 위한 기본 제공 Zero Trust

Zero Trust를 인터넷으로 확장

방대한 공격 표면, 제한된 제어

오늘날 웹 브라우저는 가장 많이 사용되는 기업 애플리케이션이며, 방대한 공격 표면을 가지고 있습니다.

그러나 지금까지 사용자를 브라우저 기반 위협으로부터 완벽하게 보호하지 못했습니다. 또한 사용자가 중요한 데이터와 상호 작용하는 방법을 보호하기 위해 제어 수단을 적용하는 것이 그 어느 때보다 더 어려워졌습니다.

Zero Trust 완성

Zero Trust를 브라우저에 추가하면 기본적으로 장치에서 실행되는 코드나 상호작용을 신뢰하지 않습니다.

Cloudflare 브라우저 격리는 에지에서 모든 코드를 실행하여, 신뢰할 수 없는 웹 콘텐츠로부터 사용자를 격리하고 신뢰할 수 없는 사용자와 장치가 수행하는 브라우저 상호작용으로부터 데이터를 보호합니다.

평범한 원격 브라우저가 아닙니다

- 호환성은 모든 웹 페이지 및 브라우저에서 기본적으로 작동합니다.
- 성능에 따라 낮은 웹 페이지 대기 시간 스트림이 제공됩니다.

사용하고 있는 데이터를 신뢰할 수 없는 사용자와 장치로부터 보호하고 제로 데이 공격을 포함한 랜섬웨어와 피싱으로부터 장치와 사용자를 안전하게 보호하세요.

설치할 필요가 없으니 지금 사용해 보세요

볼트온이 아닌 내장형 보안

Cloudflare에서 구축

Cloudflare의 브라우저 격리는 네트워크상의 다른 Zero Trust 서비스와 함께 완전하게 구축되었고 275개 이상의 위치에서 실행되도록 고안되었습니다.

웹 브라우징 세션은 사용자에게 최대한 가까운 곳에서 제공되어 번개처럼 빠른 경험을 보장해 줍니다.

기본 통합

다른 공급자와는 달리, Cloudflare는 모든 Zero Trust 서비스와 브라우저 격리 기능을 기본 통합했습니다.

다음을 위해 단일 관리 인터페이스를 사용해 보세요.

- 보안 웹 게이트웨이(SWG)
- Zero Trust 네트워크 액세스(ZTNA)
- 클라우드 액세스 보안 브로커(CASB)
- 클라우드 이메일 보안(로드맵에 포함)
- ...기타 등등

공격 표면 축소
Zero Trust 브라우징은 분류되지 않은 사이트, 위험한 사이트, 심지어는 위험성이 낮은 사이트에 존재하는 악성 코드가 사용자 장치를 감염시키지 않도록 차단합니다.

배포 단순화
애플리케이션 액세스를 관리하는 곳과 동일한 장소에서 Zero Trust 브라우징 정책을 설정합니다.

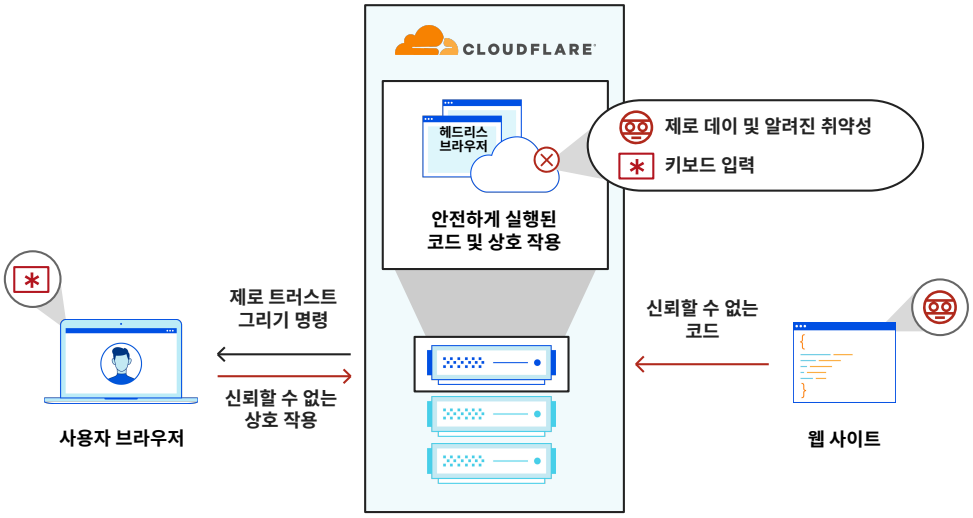
데이터 보호
앱이나 위험한 사이트에서 사용자 작업(키보드 입력, 복사, 인쇄, 업로드/다운로드)을 제어하여 데이터 손실과 피싱을 방지합니다.

사용자 경험에 손상을 입히지 않으면서 공격 표면을 축소시킵니다

과제:
그 어떤 IT 팀도 알려진 취약성에 대해 모든 브라우저를 패치할 수는 없습니다. 또한 실질적으로 최상의 지능을 사용하더라도 필터링과 검사로는 위협을 100% 방지하거나 감지할 수는 없습니다. 모든 사이트를 차단하는 것도 해결책이 아닙니다. 과도하게 제한하면 사용자 생산성이 떨어지므로 더 큰 피해를 입을 수 있습니다.

솔루션:
브라우저 격리는 Chromium 브라우저의 헤드리스 버전을 실행하여 엔드포인트가 아니라 에지에서 모든 브라우저 코드를 렌더링하므로 맬웨어와 같은 알려진 위협과 알려지지 않은 위협이 완화됩니다. 짧은 대기 시간으로 최종 사용자에게 보이지 않으며 로컬 브라우저처럼 느껴집니다.

작동 방식



장치 클라이언트를 *사용한* 배포
완벽한 L4-7 필터링 및 검사를 위해 사용자 트래픽을 장치에서 Cloudflare 전역 네트워크로 전송합니다.

클라이언트리스 배포
공용 IP 또는 장치를 사이트에 있는 잠재적인 악성 코드에 노출시키지 않고 사용자를 격리된 하이퍼링크로 전송합니다.

주요 사용 사례

랜섬웨어

격리 기능은 랜섬웨어 감염을 효과적으로 막아줍니다. 하지만, 위험한 사이트와 도메인을 차단해주는 SWG, 위협의 내부망 이동을 줄여주는 ZTNA와 같은 서비스를 이용하면 격리되지 않은 사이트에서도 이러한 방어 방식을 강화할 수 있습니다.

피싱 및 이메일 보안

격리 기능은 피싱 링크의 유해한 코드가 로컬에서 실행되지 않도록 막아주며, 중요한 개인 정보가 키보드로 입력되지 않도록 방지하기도 합니다. 이와 더불어 관리자가 Area 1을 통해 클릭 한 번으로 이메일 필터링을 활성화할 수 있는 기능도 곧 공개됩니다.

제로 데이 공격

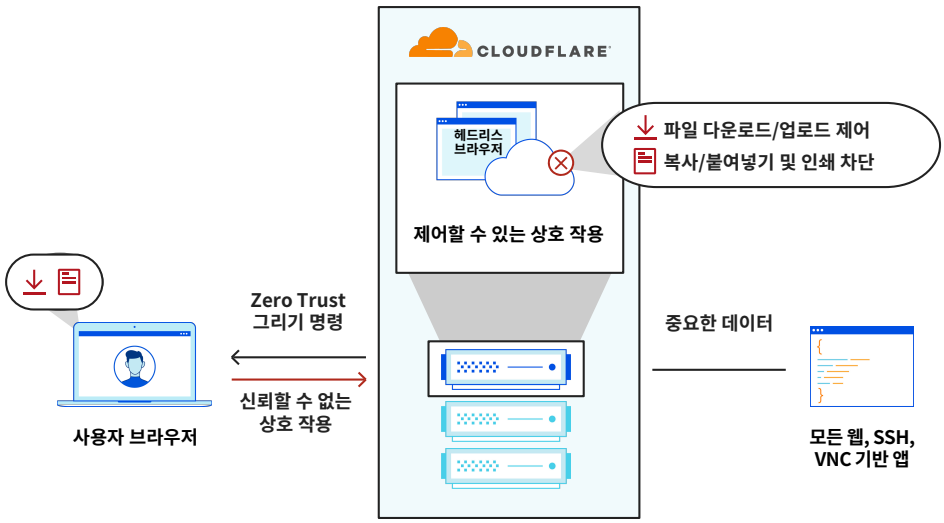
제로 데이 취약성에 대한 패치를 사용할 수 있는 경우 Cloudflare에서는 네트워크 상 모든 원격 브라우저에 자동으로 배치를 배포합니다. 즉, 관리자는 장치를 보호하면서 사용자의 작업을 방해하지 않고 업데이트를 시행할 수 있습니다.

웹 브라우저에서 사용 중인 데이터 보안

과제:
SaaS 소프트웨어의 부상으로 인해 웹 브라우저는 사용자가 데이터에 액세스하는 기본적인 방법이 되었습니다. 그러나 전통적으로 데이터가 브라우저에 전송되면 이에 대한 관리자의 제어가 제한되었습니다. 사용자는 일반적으로 중요한 데이터 또는 PII를 다른 웹 사이트, 앱, 위치에 복사, 붙여넣기, 인쇄를 할 수 있습니다. 이러한 일반적인 작업으로 인해 데이터 유출의 위험이 증가합니다.

솔루션:
격리된 브라우저를 실행하면 관리자가 제어력을 되찾으므로, 웹 사이트나 SaaS 애플리케이션에서 중요한 데이터를 보호할 수 있습니다. 관리자는 단 몇 번만 클릭하여 브라우저에서 위험한 사용자 행동을 방지하는 세밀한 규칙을 구축할 수 있습니다. 이 규칙에는 다운로드, 업로드, 복사 및 붙여넣기, 키보드 입력, 프린트 기능 등의 제한이 포함됩니다.

작동 방식



장치 클라이언트를 *사용한* 배포
사용자가 관리형 장치에서 데이터와 상호 작용하는 것에 대한 완벽한 가시성을 확보하고 장치 상태를 인식하는 정책을 만들어 보세요.

클라이언트리스 배포
사용자가 비관리형 장치에서 정기적으로 액세스할 확률이 가장 높은 중요한 데이터를 포함한 앱(예: CRM)을 격리하세요.

주요 사용 사례

협력업체 액세스 보호

사용자 장치에 어떤 소프트웨어도 설치하지 않고 특정 하이퍼링크에 대한 연결을 격리합니다.

이 클라이언트리스 모델을 이용해 구성 오버헤드를 추가하지 않고도 협력업체가 비관리형 장치를 통해 상호작용하는 데이터를 보호합니다.

의심스러운 사이트에서 입력 제어

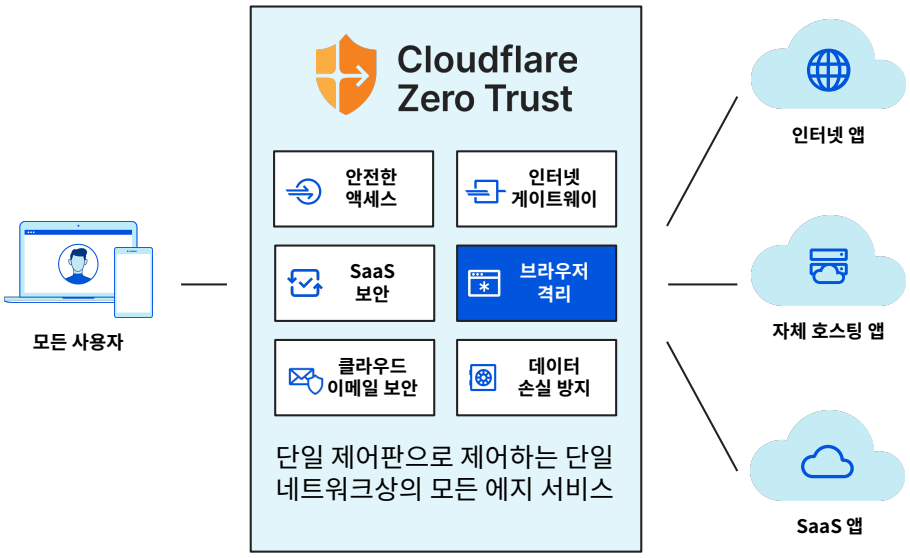
관리자는 피싱에 자주 사용되는 '타이포스쿼팅' 및 '도메인'과 같은 위험성이 높은 웹 사이트를 격리하여 팀을 보호할 수 있습니다. Cloudflare 는 읽기 전용 모드에서 서비스를 제공하고 파일 업로드, 다운로드, 키보드 입력을 비활성화합니다.

타사 솔루션과 통합

관리자는 Cloudflare의 클라이언트리스 배포를 통해 Cloudflare를 기존 웹 또는 이메일 게이트웨이와 통합시켜 레거시 서비스를 점차 대체해 나갈 수 있습니다. 원격 브라우저로 위험성이 높은 클릭을 전송하고 사용자 정의 차단 페이지 또는 기타 보호 기능을 적용합니다.

브라우저 격리: Zero Trust의 기본

격리는 Zero Trust의 핵심 원칙입니다. 브라우저에 대한 가시성과 제어를 Cloudflare Zero Trust 플랫폼에서 몇 번의 클릭만으로 쉽게 확장할 수 있습니다.



접근이 쉬워진 격리
이제까지 브라우저 격리는 높은 비용과 복잡성으로 인해 대기업만 구매할 수 있는 독립형 솔루션이었습니다.

Cloudflare를 이용하면 ZTNA, SWG, 기타 SSE 서비스와 기본 통합되므로 브라우저 격리로 Zero Trust를 추가적으로 확장하기 전에 거쳐야 하는 보안 최신화 여정을 쉽게 시작할 수 있습니다.

로컬 및 원격 브라우징 비교

로컬 브라우징
신뢰할 수 없는 웹 페이지 코드 및 피싱 사이트가 엔드포인트 장치의 로컬에서 실행됩니다. 사용자가 거리낌 없이 중요한 데이터를 피싱 웹 사이트와 자신의 장치에 입력하면 데이터가 직접적으로 패치되지 않은 취약점이나 제로데이 위협에 노출됩니다.

원격 브라우징
필터링되지 않은 코드나 사이트를 지속적으로 패치된 원격 브라우저에서 실행될 수 있습니다. 사용자 상호 작용을 제어하여 맬웨어와 피싱 공격을 방지하며 제로 데이 공격은 최종 사용자의 장치에서 멀리 떨어진 곳에서 격리됩니다.

Cloudflare의 접근법

네트워크 벡터 렌더링(NVR)
대역폭이 많이 사용되는 픽셀 푸시 또는 취약한 콘텐츠 무해화 및 재구성 기술과는 달리 NVR은 어떠한 악의적 웹 페이지 코드를 전송하거나 최종 사용자 경험에 영향을 주지 않은 채로 장치에 안전한 그리기 명령을 스트리밍합니다.

Cloudflare의 전역 네트워크
다른 공급자는 원격 브라우저를 공용 클라우드 공급자에서 호스팅합니다. Cloudflare는 브라우저를 사용자에게 더 가까이 이동시켜 어디서든 로컬 브라우징과 다름없는 경험을 선사합니다.

주요 기능

- 모든 브라우저 코드를 사용자와 멀리 떨어진 클라우드에서 실행
- 픽셀 푸싱 없음
- 초고속 네트워크(전 세계 인터넷 사용자의 95%로부터 최대 50밀리초 거리)
- 모든 최신 브라우저와 호환 가능
- 장치 클라이언트 유무와 상관없이 배포
- 데이터가 기업 앱을 벗어나지 않도록 보호하고 섀도우 IT 가시성을 확보
- Cloudflare의 네트워크 방화벽과 Zero Trust 규칙의 인텔리전스를 이용해 위협 차단
- 100% 가동 시간 SLA

더 빠르고 안전한 브라우징을 오늘 경험해 보세요

Browser Isolation을 지금 사용해 보세요