CLOUDFLARE

제품 요약

Cloudflare Zero Trust

가장 빠른 Zero Trust 브라우징 및
애플리케이션 액세스 플랫폼

경계를 넘어선 위험

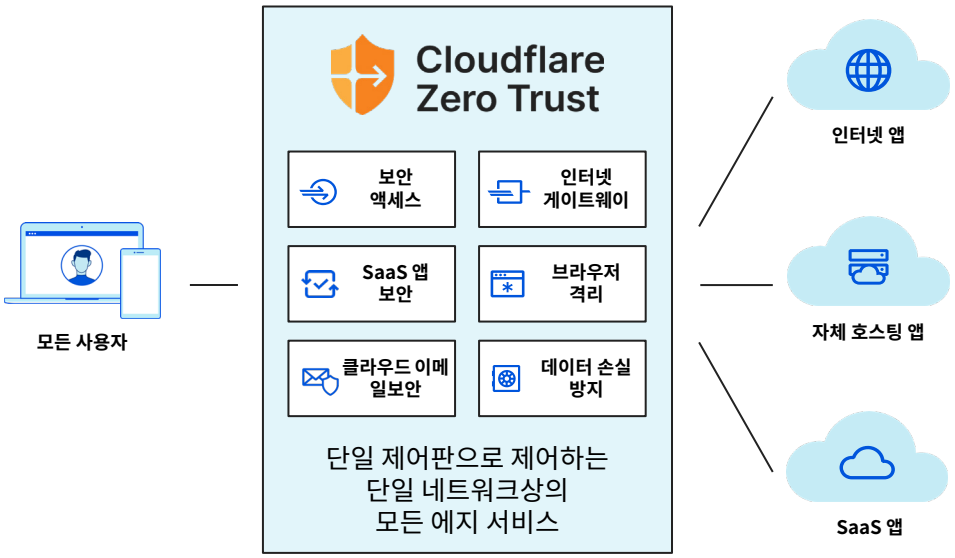
애플리케이션과 사용자가 기업 경계의 벽을 넘게되면 보안 팀은 데이터를 어떻게 안전하게 보호할 것인지를 두고 차단과 허용 사이에서 항상 타협을 해야 했습니다. 트래픽 보호를 위한 위치 기반 방식(VPN, 방화벽, 웹 프록시 등)은 그 부담 속에 무용지물이 되어 버렸고, 이에 따라 기업은 가시성이 제한되고 구성이 상충되며 과도한 위험에 노출되는 환경에 놓이게 되었습니다.

위험이 어디에나 존재하는 지금, 기업은 클라우드에서 제공되는 Zero Trust를 채택하는 쪽으로 선회하고 있습니다.

인터넷 네이티브 Zero Trust 채택

Cloudflare Zero Trust는 원격 및 사무실 근무자가 응용 프로그램 및 인터넷에 접속할 때 가시성을 높이고 복잡성을 제거하며 위험을 줄여주는 보안 플랫폼입니다. 싱글 패스 아키텍처로 트래픽을 확인하고 필터링하며 검사하고 위협에서 격리합니다.

Cloudflare의 Zero Trust는 100여 개 국가의 275개 이상의 도시에 걸쳐 있는 세계에서 가장 빠른 Anycast 네트워크에서 실행되므로 다른 공급자에 비해 배포는 더욱 빠르고 성능은 더욱 우수합니다.



보안 액세스
어떤 장치, 어떤 위치에서든 모든 사용자와 앱 간의 액세스를 단순화하고 보호

위협 방어
사용자와 데이터를 웹, 이메일, 다중 채널 위협으로부터 안전하게 보호

Microsoft로 보호
Microsoft, Google 등에서 이용할 수 있는 모든 SaaS 제품군 가시성 및 제어

하이브리드 근무 보호
팀 생산성 개선, 사이버 위험 절감, 기술 효율성 개선

비즈니스 이점

과도한 신뢰 감소

ID 및 컨텍스트 기반 Zero Trust 규칙을 이용해 앱을 보호하세요. 피싱, 랜섬웨어, 기타 온라인 위협을 차단하세요. 신뢰할 수 없는 코드를 장치에서 분리하고 신뢰할 수 없는 사용자 활동을 데이터와 분리하여 엔드포인트를 위험으로부터 격리하세요.

복잡성 제거

레거시 포인트 제품에 대한 의존도를 줄이는 동시에, 그 연결이 어떻게 시작되는지 또는 트래픽이 네트워크 스택 어디에 존재하는지에 상관없이 모든 트래픽에 표준 보안 컨트롤을 적용할 수 있습니다.

가시성 복원

DNS, HTTP, SSH, 네트워크, 셰도우 IT 활동에 대한 포괄적인 로그로써 모든 앱에 걸쳐 사용자 활동을 모니터링하고, 선호하는 여러 클라우드 스토리지 및 분석 도구로 로그를 전송합니다.

보안 액세스(ZTNA)

모든 사용자와 모든 애플리케이션을 연결하는 더 빠르고 간편하고 안전한 방법

문제: 느리고 복잡하며 위험한 액세스

전통적인 경계 기반 액세스 제어(예: VPN)는 점점 골칫거리가 되어 가고 있습니다. 성능이 느려 최종 사용자의 생산성이 떨어지고, 다루기 까다로운 구성 때문에 관리자는 애를 먹고 있으며 내부망 이동을 포함하기가 어렵습니다.

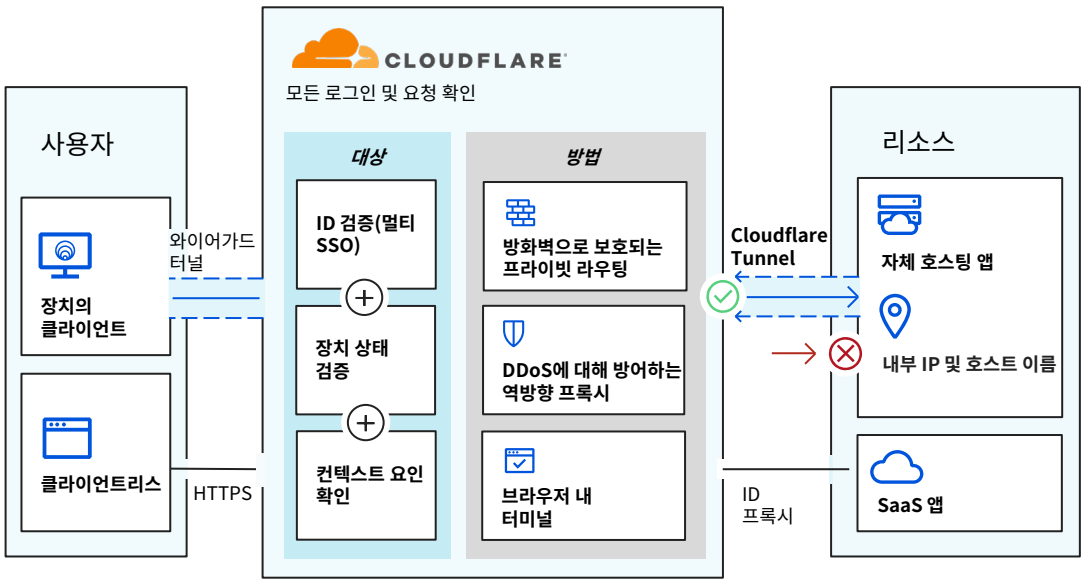
클라우드 채택과 하이브리드 작업이 가속화되면서 이러한 결점이 더욱 두드러지고 VPN은 더욱 취약해졌습니다.

Zero Trust 네트워크 액세스(ZTNA)

Cloudflare ZTNA 서비스인 Access는 온프레미스 네트워크에 있든, 공용 클라우드 또는 SaaS 환경에 있든 모든 애플리케이션을 보호함으로써 VPN 클라이언트를 보강하거나 아예 대체합니다.

Cloudflare ZTNA는 귀사의 ID 공급자 및 엔드포인트 보호 플랫폼과 연동하여 거부를 기본으로 하는 Zero Trust 규칙을 적용하여 기업 애플리케이션, 비공개 IP 공간, 호스트 이름에 대한 액세스를 제한합니다.

작동 방식



클라이언트리스 배포
브라우저를 통해 액세스 가능한 웹 기반, SSH 기반 또는 VNC 기반 셀프 호스팅 앱 배포.

Cloudflare의 장치 클라이언트를 통한 배포
내부 IP, 호스트 이름 및 비-웹 앱에 연결.

주요 사용 사례

원격 근무 및 BYOD 이니셔티브 지원

사용자가 어디에 있든 ID, 장치 상태, 인증 방법, 기타 상황 요인을 기반으로 모든 사용자에 대한 액세스를 검증할 수 있습니다.

하이브리드 인력에 대해 Zero Trust 정책을 시행하고, 관리형 및 비관리형 장치를 모두 보호함으로써 Bring-Your-Own-Device(BYOD) 이니셔티브를 지원할 수 있습니다.

유연성을 통해 타사 액세스 간소화

계약업체, 공급업체, 에이전시, 협력업체 등을 위한 액세스 설정 속도를 높일 수 있습니다.

여러 ID 공급자(IDP)를 한꺼번에 온보딩하고, 이미 사용 중인 IDP를 기반으로 최소한의 권한 규칙을 설정할 수 있습니다.

SSO 라이센스 프로비저닝, VPN 배포, 단발성 사용 권한 생성을 피할 수 있습니다.

관리 구성 및 지원 간소화

단 몇 분이면 새 사용자, ID 공급자, Zero Trust 규칙을 추가할 수 있습니다.

직원 온보딩 시간을 단축하고(eTeacher Group) IP 기반 액세스 구성에서 벗어나(BlockFi) 새로운 생산성을 확보할 수 있습니다. VPN 관리를 위한 전담 직원을 채용할 필요도 없습니다(ezCater).

위협 방어(SWG 및 RBI)

인터넷으로 향하는 트래픽을 필터링하고 검사하며 격리

문제: 진화하는 위협 환경

사용자 생산성을 유지하면서 보안을 강화하는 일은 그 어느 때보다 까다롭습니다. 원격 근무를 하게 되면 중요한 데이터를 로컬에 저장하는 비관리형 장치가 더 많아지게 됩니다. 그 와중에 랜섬웨어, 피싱, 셰도우 IT, 기타 인터넷 기반의 위협은 그 규모와 정교함이 폭발적으로 증가하고 있습니다.

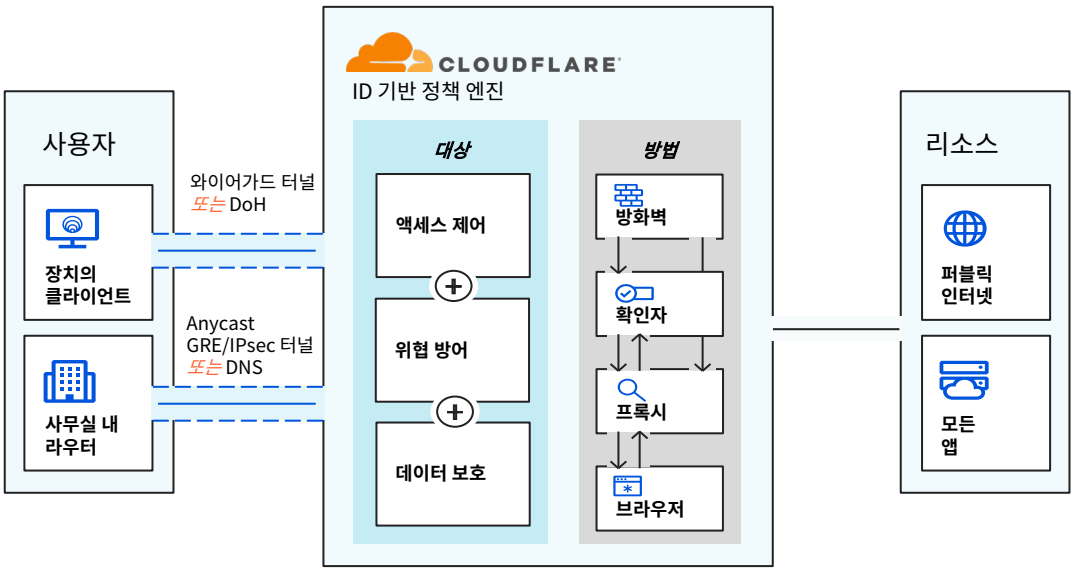
기존의 포인트 솔루션과 데이터 백업에 의존해 다중 채널 위협에 대항하는 것은 아주 위험한 전략입니다.

Zero Trust 브라우징의 SWG

당사의 Secure Web Gateway(SWG)인 Cloudflare Gateway는 ID 기반 웹 필터링과 기본 통합되어 있는 원격 브라우저 격리(RBI)를 이용해 사용자를 보호합니다.

빠른 가치 창출을 달성할 수 있는 원격 또는 사무실 사용자용 DNS 필터링을 시작하세요. 그다음, 보다 포괄적인 HTTPS 검사를 적용하고, 최종적으로 RBI 컨트롤을 확장해 모든 인터넷 활동을 대상으로 Zero Trust를 구현하세요.

작동 방식



더 이상 백홀은 없습니다.
레거시 장비 대신 Cloudflare를 통해 L4-7 트래픽을 전송하세요.

필터, 검사 및 격리를 인터넷으로 향하는 트래픽과 내부 리소스 트래픽 모두에 적용할 수 있습니다.

주요 사용 사례

랜섬웨어

당사의 글로벌 네트워크 인텔리전스를 기반으로 랜섬웨어 사이트 및 도메인을 차단합니다. 위험한 사이트에서의 브라우징을 격리하여 보호 성능을 강화합니다.

SWG 필터링과 자동 거부형의 RBI, ZTNA와 통합하여 랜섬웨어가 네트워크에서 래터럴하게 확산되고 권한을 에스컬레이션할 위험을 완화합니다.

피싱 차단

알려진 피싱 도메인 및 '새로운' / '새롭게 발견된' 피싱 도메인을 필터링합니다. 브라우징을 격리하여 유해한 페이로드가 로컬에서 실행되는 것을 방지합니다. RBI의 키보드 입력 컨트롤을 통해 의심스러운 피싱 사이트에서 중요한 정보가 제출되는 것을 방지합니다.

또한, 관리자가 Area 1을 통해 클릭 한 번으로 이메일 필터링을 활성화할 수 있는 기능도 곧 공개됩니다.

데이터 누출 방지

파일 유형 제어와 함께 데이터 손실 방지(DLP)를 실행하여 사용자들이 사이트에 파일을 업로드하지 못하게 하세요.

Zero Trust 브라우징을 배포하여 웹 기반 앱 내부에 있는 데이터를 제어하고 보호하세요. 다운로드, 업로드, 복사 및 붙여넣기, 키보드 입력, 프린트 기능 등의 브라우저 내 사용자 작업을 제어하세요.

Microsoft로 보호(CASB)

가시성 및 컨트롤 증가와 오버헤드 감소를 위해 SaaS 보안 간소화

문제: SaaS 앱 급증

현대의 인력은 그 어느 때보다, Microsoft 365와 같은 SaaS 애플리케이션에 크게 의존하고 있습니다. 하지만 각각의 SaaS 앱은 보안 요건이 서로 다르며 전통적인 보안 경계의 보호 장치 밖에서 작동합니다.

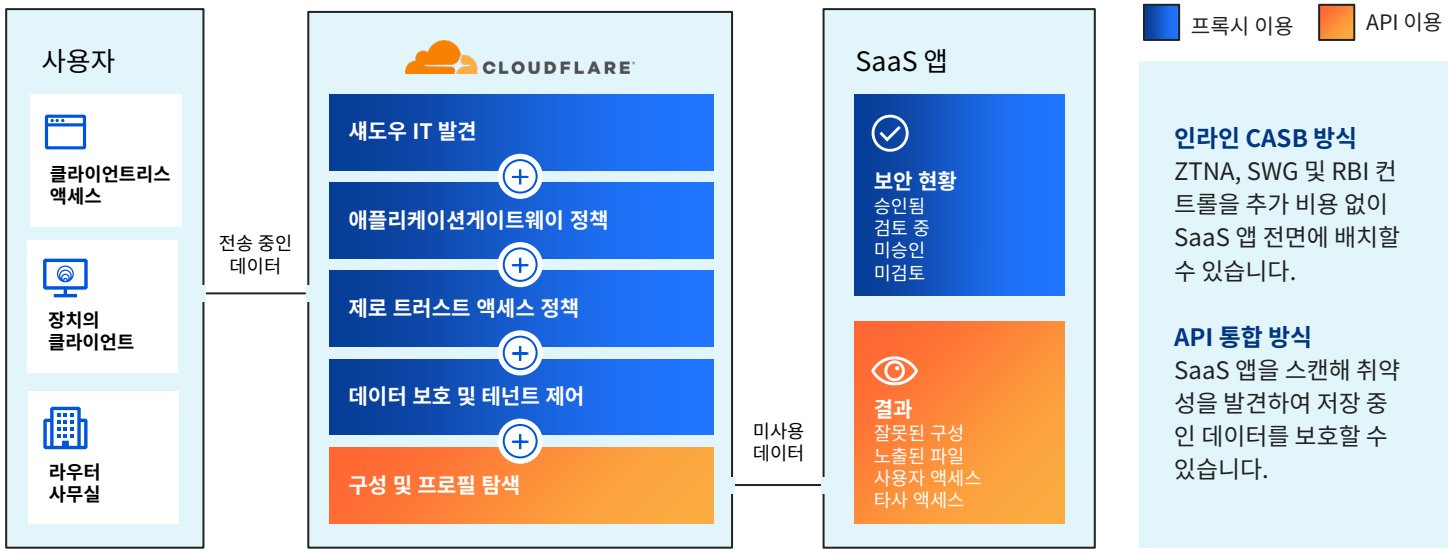
많은 기업에서 수십 가지 SaaS 앱을 도입하면서 점점 더 일관된 보안, 가시성, 성능을 유지하기 어려워 하고 있습니다.

클라우드 액세스 보안 브로커(CASB)

Cloudflare의 CASB 서비스는 SaaS 앱에 대한 포괄적인 가시성과 컨트롤을 제공하기 때문에 데이터 누출과 규제 위반을 쉽게 방지할 수 있습니다.

내부자 위협, 위험한 데이터 공유, 악성 사용자를 차단할 수 있습니다. 모든 HTTP 요청을 기록해 비승인 SaaS 애플리케이션을 파악하고, SaaS 앱을 검사하여 잘못된 구성과 의심스러운 활동을 감지하세요.

작동 방식



주요 사용 사례

테넌트 및 데이터 보호 제어 적용

HTTP 게이트웨이 정책을 통해 테넌트 컨트롤을 적용하여 사용자가 부주의에 의해서든 악의적인 의도에 의해서든 인기 SaaS 앱의 잘못된 버전에서 데이터에 액세스하고 데이터를 저장하지 않도록 방지합니다.

웹 기반 SaaS 애플리케이션 내 사용자 작업(복사/붙여넣기, 다운로드, 인쇄 등)을 제어하여 데이터 손실 위험을 최소화합니다.

섀도우 IT 완화 및 제어

비승인 SaaS 애플리케이션으로 인한 위험을 최소화합니다.

Cloudflare는 활동 로그 내 모든 HTTP 요청을 수집하고 애플리케이션 유형별로 자동 분류합니다. 그러면 관리자는 그 상태를 설정하고, 기업의 승인 앱과 비승인 앱의 사용 정보를 모두 추적할 수 있습니다.

새로운 위협 및 잘못된 구성 식별

API를 통해 인기 SaaS 앱(Google Workspace, Microsoft 365 등)에 연결하고 위험을 검사합니다.

사용 권한, 잘못된 구성, 부적절한 액세스, 컨트롤 문제 등 데이터와 직원을 위험에 빠트릴 수 있는 문제에 대한 가시성을 제공하여 IT 및 보안팀에 힘을 실어주세요.

피싱 방어(CES)

포괄적인 위협 방어를 위해 이메일로 Zero Trust 확장

문제: 위협 벡터 1위가 바로 이메일

이메일은 팀의 1순위 커뮤니케이션 방식인 동시에 공격자들이 1순위로 사용하는 공격 방식이기도 합니다. 실제 최근 연구에서는 사이버 공격 중 91%가 피싱 이메일로 시작된다는 결과가 나왔습니다.

공격자는 이메일 커뮤니케이션에 부여되곤 하는 높은 수준의 신뢰를 겨냥해 악용하는 경우가 많습니다.

클라우드 네이티브 이메일 보안 통합

Area 1 클라우드 이메일 보안(CES)이 포괄적인 Zero Trust 전략의 일부에 포함되면서, 이메일에서 암시적 신뢰가 사라져 피싱 및 비즈니스 이메일 손상(BEC) 공격을 선제적으로 방어할 수 있게 되었습니다.

이메일 등 모든 사용자 트래픽을 검증, 필터링, 검사하며, 알려진 위협과 알려지지 않은 모든 위협으로부터 격리합니다. Area 1은 고객이 이메일로 인한 위협을 차단하고, 예방적인 보안 상태를 도입하고, 피싱 사고 응답 시간을 90% 단축할 수 있도록 해줍니다.

작동 원리: 모든 이메일, 웹, 네트워크 트래픽을 위한 Zero Trust

주요 사용 사례

BEC 및 이메일 기반 사기 방지

감정 분석, 파트너 소셜 도식화, 메시지 분류, 캠페인 소스 분석을 통한 정교한 비즈니스 이메일 손상(BEC) 공격과 공급자 계정 탈취를 막습니다.

사기성 금융 커뮤니케이션을 자동으로 차단하고, 격리하고, 에스컬레이션합니다.

다중 채널 공격으로부터 보호

이메일 및 웹과 같은 다양한 커뮤니케이션 채널을 통해 개인을 겨냥하는 공격 캠페인을 쉽게 차단하므로, 사용자는 격리된 원격 브라우저에서 의심스럽거나 알 수 없는 링크를 안전하게 로드할 수 있습니다.

클릭 시 작동하는 링크 분류를 통해, 전달 이후 링크를 무기로 사용하는 지연 피싱 공격을 잡아냅니다.

피싱 분류 및 대응 가속화

보안 조사 사이클에서 자유로워지고, 이메일 환경에 대한 인사이트를 확보하며, 피싱 위협을 빠르게 무력화할 수 있게 기존 팀을 강화하는 전용 리소스로 응답 시간을 줄여줍니다.

관리형 이메일 보안 서비스를 통해 추가적인 지원 및 보안 전문 지식을 얻어보세요.

하이브리드 근무 보호: Cloudflare의 차이점

현대 인력을 위한 최신 보안

배포 단순성

Cloudflare는 쉽게 설정하고 운영할 수 있는 균일하고 구성 가능한 플랫폼을 제공합니다. 소프트웨어 전용 커넥터 및 일회성 통합을 통해 Cloudflare 온램프 및 에지 서비스는 모두 연동됩니다.

덕분에 IT 담당자와 최종 사용자 모두 더 나은 경험을 누릴 수 있습니다.

네트워크 복원력

Cloudflare의 종단 간 트래픽 자동화는 모든 위치에서 일관된 보호와 함께 안정적이고 확장 가능한 연결을 보장합니다.

Cloudflare의 경우, 모든 에지 서비스가 다른 보안 공급자와 달리 모든 네트워크 위치에서 모든 고객이 이용할 수 있도록 구축되었습니다.

혁신 속도

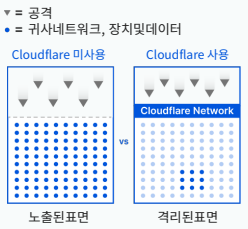
당사의 미래 지향적인 아키텍처를 통해 매우 신속하게 새로운 보안 및 네트워킹 성능을 구축하고 제공할 수 있습니다.

새로운 인터넷 및 보안 표준의 발빠른 채택이든 고객 주도 사용 사례 구축이든, 당사의 기술 역량은 그 자체로 더 이상의 설명이 필요 없는 기록이며, 이를 통해 만든 탄탄한 기초는 궁극의 기회를 제공합니다.

Zero Trust를 통해 비즈니스의 시간과 돈을 절약하는 5가지 방법

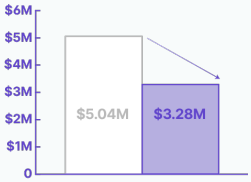
공격 표면 감소

91% ↓



침해 비용 감소

35% ↓



직원 온보딩 가속화

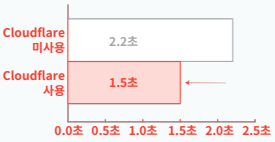
60% ↑

IT 티켓 부담 감소

80% ↓

사용자 대기 시간감소

39% ↓



사용성 최적화

단일 관리 인터페이스

애플리케이션과 인터넷 액세스 정책 모두에 대해 기본 내장 대시보드를 이용하여 구성을 간소화합니다.

단일 대시보드를 이용하여 ID 공급자, 엔드포인트 보호 및 네트워크 온램프와 통합합니다.

단일 통합 플랫폼

단일 플랫폼과 단일 제어판으로 VPN 클라이언트, 온프레미스 방화벽, 기타 포인트 보안 솔루션의 패치워크를 대체합니다.

보안을 에지로 옮겨 비용과 복잡성을 줄입니다.

비교를 불허하는 사용자 경험

Cloudflare는 전 세계 100여 개 국가의 275개 이상 도시에 걸쳐 있는 방대한 Anycast 네트워크에서 최적화된 인텔리전스 기반 라우팅을 이용하여 사용자 및 서비스와 더 가까운 위치에서 요청을 더 빠르게 라우팅합니다.

Zero Trust 여정을 가속화하세요

지금 사용해 보세요.

문의