프라이빗 라우팅을 이용하는 Zero Trust 네트워크 액세스

수평 이동을 방지하고 VPN 의존도를 낮춥니다

응용 프로그램 액세스를 위해 네트워크 기반 제어(VPN 및 IP 위치 제한)를 신뢰하면 공격 표면이 늘어나고, 가시성이 제한되며, 최종 사용자를 짜증나게 만들 수 있습니다. Cloudflare의 Zero Trust 네트워크 액세스는 여러분의 ID 공급자 및 엔드포인트 보호 플랫폼과 함께 작동하여 기업 응용 프로그램, 내부 IP 공간, 호스트 이름에 대한 액세스를 제한하는 기본값으로 거부하는 Zero Trust 규칙을 시행합니다. Cloudflare의 방대하고 성능 기준에 맞는 Anycast 네트워크를 통해 사용자 연결이 VPN보다 더 빨라집니다.

Cloudflare에서 내부적으로 Zero Trust 네트워크 액세스를 배포한 후 다음과 같은 효과가 있었습니다.

- 공격 표면 91% 감소[1]
- IT 부문의 노력을 줄여 비용 2배 절감
- VPN 관련 티켓 처리 시간 80% 단축
- 티켓 수 70% 감소
- 신규 직원 온보딩 시 생산적인 일에 투입할 수 있는 시간 연간 300시간 이상 증가

Access로 할 수 있는 일들

모든 응용 프로그램 보호

Cloudflare는 ID 및 응용 프로그램 모두에 구애받지 않으므로, 선호하는 ID 공급자를 통해 어떤 응용 프로그램, SaaS, 클라우드 또는 온프레미스 환경이든 보호할 수 있습니다.

클라이언트 유무에 관계없이 사용자를 유연하게 연결

클라이언트 소프트웨어나 최종 사용자 구성이 필요 없는 웹 앱 및 SSH 연결을 지원합니다. 웹 기반이 아닌 응용 프로그램, RDP 연결, 프라이빗 라우팅에 대해서는 인터넷 및 응용 프로그램 액세스 사용 사례 전반을 포괄하는 단일 클라이언트를 활용합니다.

여러 ID 공급자 간의 ID 페더레이션 활성화

모든 기업 ID 공급자(Okta, Azure AD 등)를 통합하여 보다 안전한 마이그레이션, 획득, 서드파티 사용자 액세스를 구현합니다. 임시 액세스를 제공하는 일회용 PIN을 활성화하거나 LinkedIn 및 GitHub와 같은 소셜 ID 소스를 통합니다.

기업 리소스 간의 수평 이동 제한

IP 방화벽 및 Zero Trust 규칙으로 레거시 응용 프로그램에도 강력하고 일관된 인증 방법을 적용합니다.

장치 인식 액세스 시행

리소스에 대한 액세스 권한을 부여하기 전에 게이트웨이 클라이언트, 일련번호, mTLS 인증서를 포함하는 장치 상태를 평가하여 오직 안전하고 알려진 장치만 기업 리소스에 연결할 수 있도록 합니다. Crowdstrike, Carbon Black, Sentinel One, Tanium 등 여러 엔드포인트 보호 플랫폼(EPP) 공급자로부터의 장치 상태를 통합합니다.

모든 앱에 걸쳐 사용자 활동 기록

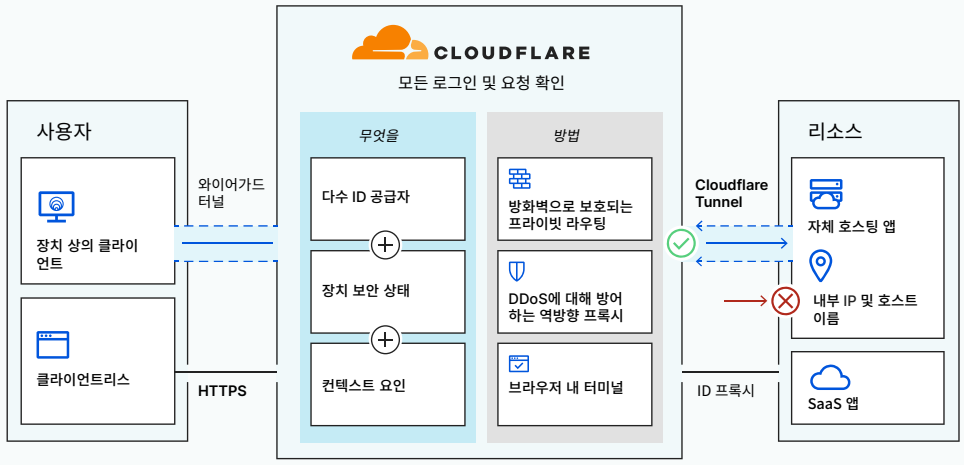
보호된 응용 프로그램에 대해 로그인과 로그아웃뿐 아니라 모든 요청을 로그에 기록합니다. Cloudflare에서 활동 로그를 집계하거나 SIEM 공급자에게 내보냅니다.

[1]Zero Trust 네트워크 액세스를 인터넷 브라우징과 결합하였을 때

Cloudflare의 차별성

- **타의 추종을 불허하는 성능**으로 Cloudflare의 Anycast 네트워크로 최적화된 인텔리전스 기반 라우팅을 통해 요청을 더 빠르게 라우팅합니다. 평균적으로 웹 앱 액세스 속도가 30% 더 빨라지며 TCP 연결 왕복 시간이 17% 감소합니다. Cloudflare의 인텔리전스는 초당 2,500만 개의 HTTP 요청 및 초당 39,000건의 새로운 TCP 연결의 네트워크 데이터 분석을 기반으로 합니다.
- **더 간단한 관리**로 Zero Trust 네트워크 액세스, 안전한 웹 게이트웨이, 원격 브라우저 분리 등을 관리자 경험이 포함된 하나의 제어판으로 통합합니다. 이는 처음부터 구축되었으며 여러 벤더로부터 가져오거나 짜기한 것이 아닙니다.
- **단일 패스 검사**로 트래픽을 빠르고 지속해서 전 세계에 걸쳐 확인, 필터링, 분리, 검사합니다. 모든 Cloudflare 서비스가 전 세계적으로 250여 곳의 모든 데이터 센터에 배포되기 때문입니다.

작동 방식



사용자는 VPN 대신 클라이언트나 웹 브라우저를 통해 기업 리소스에 연결합니다. 요청이 Cloudflare의 에지를 통해 라우팅되고 가속화되면, 해당 요청은 ID 공급자, 장치, 기타 컨텍스트로부터의 신호를 종합하여 판단하는 Zero Trust 규칙에 따라 평가됩니다. RDP 소프트웨어, SMB 파일 뷰어, 기타 씩 클라이언트(thick client) 프로그램의 비공개 네트워크 연결을 위해서는 VPN이 필요했던 방식을 벗어나서, 이제는 팀에서 Cloudflare의 네트워크를 통해 모든 TCP 또는 UDP 트래픽을 비공개로 라우팅하여 이를 단일 패스로 가속화, 검증, 필터링하고 성능과 보안을 향상시킬 수 있습니다.

"Cloudflare Access를 이용함으로써 자체적으로 ID 및 액세스 관리(IAM) 시스템을 개발할 필요가 없어졌습니다. Access가 보호하는 앱에 사용자 권한 기능을 구축할 필요가 없습니다. 회사의 전 직원에게 시트가 제공됩니다."

Jim Tyrrell
Canva, 인프라 책임자

"Delivery Hero에서는 언제나 고객에게 놀라운 경험을 제공하려고 노력합니다. Cloudflare Access를 이용해, 내부 직원에게도 똑같은 노력을 하고 있어요. 안전한 근무 환경을 제공하고, 세계 모든 곳에서 우리의 응용 프로그램에 접속하는 데 VPN이 필요없게 됐죠."

William Carminato
Delivery Hero, 엔지니어링 부문 선임 이사

ID 및 액세스 관리(IAM) 통합

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

엔드포인트 보호 플랫폼(EPP) 통합

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

주요 기능

일관된 정책	
사용자 지정 응용 프로그램, 프라이빗 네트워크, 인터넷 액세스 정책	**무제한**
기업 및 소셜 IdP를 통한 인증	✓
타사 통합과 Cloudflare를 활용한 장치 보안 상태	✓
기업 장치 일련번호 목록에 대한 CSV 기반 대량 가져오기	✓

가시성 향상	
활동 로그 유지	**6개월**
ID 기반 국가, 주, 장치 세부 정보 보기	✓
클라우드 스토리지 또는 SIEM으로 로그 푸시	✓

안전한 연결	
인터넷에 대한 클라이언트 기반 암호화 연결 (WARP 클라이언트)	**Win, Mac, iOS, Android**
자체 호스팅 및 SaaS 응용 프로그램에 대한 안전한 클라이언트리스 액세스	✓
자체 호스팅 응용 프로그램, 내부 IP, 호스트 이름에 대한 프라이빗 연결(Cloudflare Tunnel)	✓

단순한 상호 운용성	
엔드포인트 및 이동성 관리 통합	✓
로컬 또는 VPN 연결을 위한 분할 터널링	✓
관리되지 않는 장치를 클라이언트에서 자체 등록	✓
사용자 정의 가능한 앱 실행기	✓
다수 ID 공급자를 동시에 지원하는 인증	✓
SAML 및 OIDC를 지원하는 일반 커넥터 및 맞춤형 커넥터	✓
토큰 기반 자동화 서비스용 인증	✓
IoT및 기타 mTLS 사용 사례를 위한 인증서 기반 인증	✓

성능 저하 없음	
가동 시간 SLA	**100%**
가장 빠른 네트워크 중 하나 (250여 개의 PoP으로부터 <50 밀리초)	✓
가장 빠른 개인 정보 우선 DNS 리졸버(250개 이상의 PoP를 통해 7~31밀리초)	✓
번개처럼 빠른 정책 업데이트 (250여 개의 PoP까지 <500밀리초)	✓
번개처럼 빠른 원격 브라우저 (픽셀 푸싱 없음, 타사 클라우드가 아닌당사 네트워크에서 실행됨)	**추가 기능**

자세히 알아보고 싶으신가요?

최대 50명의 사용자까지 무료인 계정을 만들려면 www.cloudflare.com/ko-kr/products/zero-trust/access/를 방문하시기 바랍니다.