제로 트러스트 네트워크 액세스

Cloudflare Zero Trust, 특히 Access를 사용하면 팀 생산성이 높아지며, 모든 사용자가 VPN 없이 셀프 호스팅, SaaS, 비웹 앱에 액세스하므로 위험이 줄어듭니다.

하이브리드 근무를 위한 간단하고 안전한 액세스

인터넷 네이티브 제로 트러스트 네트워크 액세스(ZTNA)
요즘의 분산된 근무 환경에서는 분산된 방식으로 보안에 접근해야 합니다. 더 이상 "경계"란 없으며 VPN과 같은 기존의 원격 액세스 솔루션은 최신 보안 기대치나 성능 기대치를 충족하지 못합니다.

ZTNA는 리소스별로 ID, 장치 상태 등 세밀한 컨텍스트를 지속적으로 확인하여, 모든 위치의 모든 장비에서 모든 사용자와 앱 사이에 간단하고 안전한 액세스를 제공합니다. 완전히 새로운 이 접근 방식을 이용하면 보안과 사용자 경험 사이에서 "균형을 잡을" 필요가 없습니다. ZTNA는 두 가지 모두를 개선하여 비즈니스를 지원합니다.

또, 클라우드 마이그레이션이든, 인수 합병 활동이든, 신속한 혁신과 확장이든, 조직에서 변화에 더욱 민첩하게 잘 적응할 수 있도록 합니다. Cloudflare에서는 제로 트러스트 또는 보안 최신화 전략의 핵심으로, 프로그래밍 가능한 전역 클라우드 연결성에서 ZTNA를 제공합니다.

80% VPN 사용과 관련된 원격 액세스 지원 티켓을 해결하는 데 소요되는 평균 시간 단축 비율[1]

72% 이전 벤더 대비 월별 정책 구성에 계속 소요되는 시간 절약 비율[1]

68% 직원 및 계약자가 인증 경험 간소화로 상당한 영향을 체감한 비율[1]

최신화된 액세스로 비즈니스에 힘을 실어주세요

사용자 경험 향상

온프레미스 앱이 SaaS 앱처럼 느껴질 만큼 최신화된 보안으로 팀 생산성을 개선하세요. 느리고 투박한 VPN을 사용할 필요가 없고, 직원도 불평하지 않게 됩니다.

내부망 이동 제거

네트워크 수준 액세스 권한 대신 컨텍스트 기반, 최소 권한의 액세스를 리소스별로 부여하여 사이버 위험을 줄이고 공격 표면을 축소하세요.

손쉽게 Zero Trust 확장

중요 앱이나 가장 위험한 사용자 그룹을 보호한 다음 인터넷 네이티브 ZTNA를 넓히고 전체 비즈니스를 보호하여 기술 효율성을 개선하세요.

주요 Access 사용 사례

하이브리드 근무 보호

- ★ **VPN 강화 및 대체** — Access는 기존 VPN보다 더 빠르고 안전합니다. 핵심적인 앱을 오프로드하여 보안과 최종 사용자 경험을 개선하세요.
- ★ **계약자 액세스** — 클라이언트리스 옵션, 소셜 IdP 등으로 계약자와 같은 타사 사용자를 인증하세요.
- **개발자 액세스** — 성능을 희생하지 않고도 권한 있는 기술 사용자에게 중요 인프라에 대한 안전한 액세스를 제공하세요.

디지털 최신화 지원

- **인수합병 속도 가속화** — 기존의 네트워크 합병 방식은 모두 배제하세요. 인수합병 과정에서 다양한 IdP와 통합하고 앱별로 내부 액세스를 제공하세요.
- **클라우드 마이그레이션** — 클라우드로 앱이나 ID 디렉터리를 마이그레이션하는 것과 같이, 혁신 과정에서 비즈니스 연속성을 유지하세요.
- **피싱 차단 MFA** — FIDO2 호환 보안 키와 같은 강력한 인증을 모든 곳에 도입하세요.

VPN 강화 및 대체 시작

ZTNA 파일럿에서 중요한 앱이나 위험한 사용자를 우선시하여 VPN을 강화하세요. 웹 앱이나 브라우저 내 SSH에 클라이언트리스 액세스를 사용하여 더 신속하게 테스트하세요. VPN 전체를 대체할 수 있도록 점차 고급 기능을 도입하고, 네트워크 변화에도 동적 가시성을 유지하세요.

VPN에서 우선순위 앱 오프로드

- Cloudflare 네트워크에 내부 앱 연결
- ID 및 엔드포인트 보호 통합
- Zero Trust 규칙 구성
- 곧바로 클라이언트리스 액세스 테스트

VPN 전체 대체를 추진

- 내부 IP 및 호스트 이름에 대한 내부 DNS 확인자 지정
- 비공개 네트워크 섀도우 IT 발견을 통해 가시성 유지

계약자(타사) 액세스로 시작

관리되지 않는 장치로 인한 위험을 완화하면서 원활한 사용자 경험을 제공하세요. 간단한 계약자 인증 옵션을 구성하세요. 최종 사용자 소프트웨어가 필요하지 않습니다. 점차 고급 기능을 도입하여 추가적인 데이터 보호를 적용하세요.

클라이언트리스 액세스를 통해 타사 사용자 빠르게 연결

- 타사 사용자가 액세스해야 하는 파일럿 앱 파악
- 소셜 IdP 또는 일회용 핀으로 여러 SSO 통합
- 외부 계약자에 대한 제로 트러스트 규칙 구성
- 곧바로 클라이언트리스 액세스 테스트

데이터 보호 강화를 위해 앱 격리*

- 대기 시간이 극도로 짧은 원격 브라우저에 앱 격리
- 복사/붙여넣기또는 업로드/다운로드 차단 등, 광범위한 DLP 적용

**Zero Trust 플랫폼의 다른 부분에 걸쳐 기능 사용*

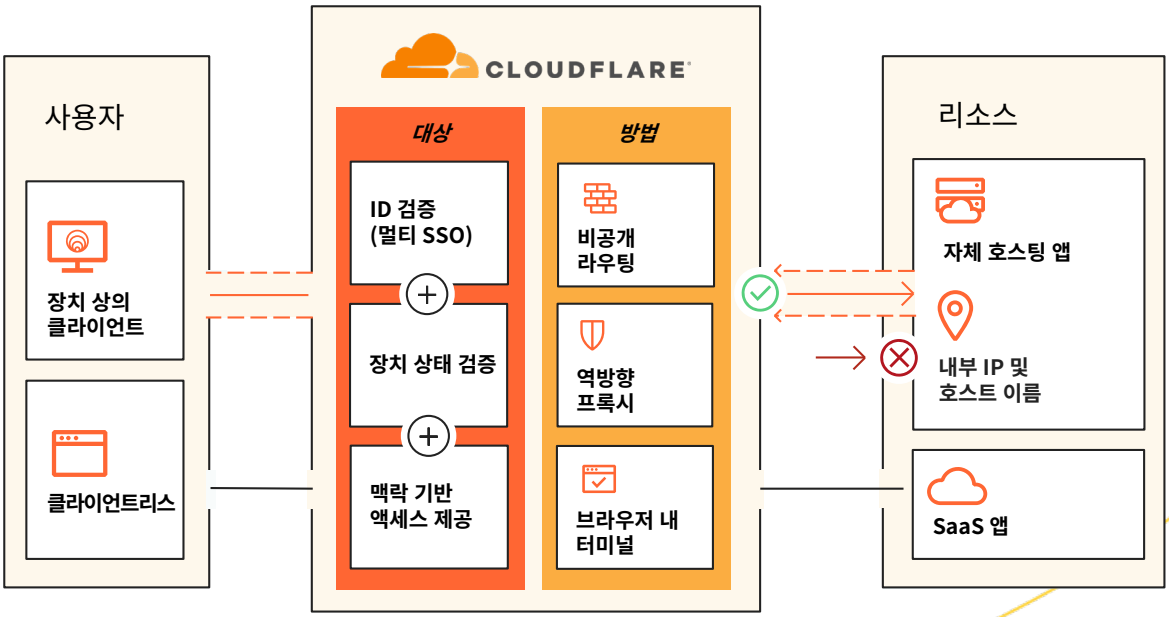
Access 작동 방식

Cloudflare Access는 ID, 장치 상태 등의 세밀한 컨텍스트를 지속적으로 확인하여 조직의 모든 리소스에 개별적으로 간단하고 안전한 액세스를 제공하고 소프트웨어로 정의된 경계를 만드는 유연한 집계 계층입니다. 사용자가 인증을 수행하고 모든 액세스 정책 기준을 충족할 경우, Access는 일정한 세션 기간 동안 유효한 서명 JSON 웹 토큰을 발급합니다. Cloudflare에서는 구성 가능한 플랫폼을 통해 모든 사용자 요청에 단일 경로 검사를 수행하며, 정책 관리 경험이 중앙화되어 있어 특별한 Anycast 네트워크 아키텍처를 통해 정책 변경 사항을 몇 초만에 전역적으로 전파합니다.

통합된 클라이언트리스 및 클라이언트 기반 작업으로 모든 장치 유형을 처리합니다. 모든 Zero Trust 서비스에 하나의 장치 클라이언트를 사용해 네트워크 트래픽을 암호화하고 고객 데이터의 개인정보 보호 상태를 유지합니다. 클라이언트리스 설정을 통해 기업 외부의 장치에 간단하고 안전한 액세스까지 제공합니다. Cloudflare의 ZTNA, DNS, 시장을 선도하는 WAF 및 DDoS 방어 서비스가 함께 작동하여, 모든 장치에서 타사 사용자와 하이브리드 인력이 액세스할 수 있는 공개 호스트 이름을 만들고 보호합니다. 또한 유저리스 인증 옵션(토큰 또는 mTLS 인증서)으로 자동화된 서비스 및 IoT 장치 사용 사례를 해결합니다.

Zero Trust 제어의 경우, 리소스는 셀프 호스팅 앱(클라우드/온프레미스) 또는 브라우저 내 SSH/VNC에 대한 역방향 프록시, SaaS 앱에 대한 ID 프록시, 비공개 서브넷 내의 모든 웹 또는 비 웹(예: 임시 TCP/UDP) 리소스에 대하여 L4-7 정방향 프록시를 통해 수행되는 클라이언트/터널 기반 비공개 라우팅에 공개 호스트 이름을 사용합니다. 전역 네트워크와 앱 연결 소프트웨어를 결합해 쿠버네티스 및 컨테이너 등의 퍼블릭 클라우드나 레거시 온프레미스 네트워크 리소스까지 모든 컴퓨팅 환경을 지원합니다. 다른 Zero Trust 벤더와 달리 VM 인프라가 필요하지 않으며 처리량 제한이 없습니다.

타사 ID, 엔드포인트, 네트워크 온램프, 로그/분석, SIEM 도구가 장치 클라이언트 및 분석용 네이티브 옵션과 함께 대시보드에 통합되어 있어, 관리자가 민첩성을 유지하면서도 이미 사용하는 도구와 함께 구축할 수 있습니다.



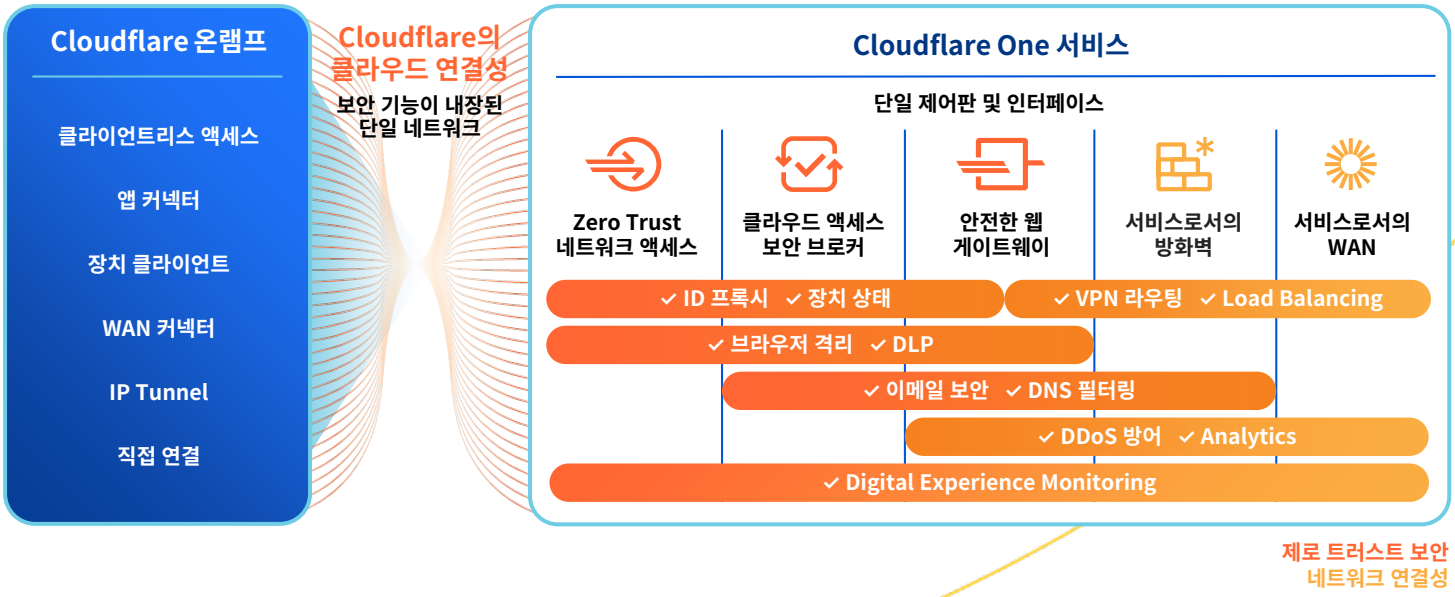
Cloudflare의 SSE 및 SASE 플랫폼의 일부인 Access

SSE 및 SASE에는 여러 해 동안의 전략적 여정이 필요한 경우가 많지만, Cloudflare에서는 여러 조직에서 ZTNA로 시작하는 경우가 많습니다. ZTNA를 사용하면 IT 팀에서 실행할 수 있고 접근할 수 있는 단계가 포함되어 있으면서도 단기적으로 상당한 비즈니스 가치가 입증되기 때문입니다. IT 리더는 하이브리드 근무를 보호하고, 위협을 방어하며, 통합하는 과정에서 데이터를 보호하려고 합니다. 신뢰할 수 있는 파트너로 Cloudflare를 선택하는 IT 리더의 수가 늘어나고 있습니다.

Cloudflare의 배포 유연성과 구성 가능한 아키텍처 덕분에 모든 조직에서는 장치, 앱, 전체 네트워크 성능을 보호하고 속도를 높여 하이브리드 인력을 보호하면서 생산성을 유지할 수 있습니다. 이를 위해 Cloudflare에서는 최종 사용자를 위한 에이전트리스 온보딩, 보호되지 않은 트래픽을 방지하기 위한 클라이언트리스 웹 격리, 관리자나 사용자의 연결 위치와 관계 없이 모든 보안 및 네트워크 서비스에서 가시성을 확보할 수 있는 통합 관리 대시보드를 지원합니다. Cloudflare의 폭넓은 전역 네트워크를 이용하면 최종 사용자에게 더 가까운 곳에서 보안 기능을 실행하고 대기 시간을 최소화하며 원활한 직원 경험을 제공할 수 있습니다. 우리의 Anycast 아키텍처는 인터넷 중단을 피해 팀의 온라인 상태를 유지하고 비즈니스 연속성을 보장하는 데 도움이 됩니다.

Cloudflare의 통합 SSE 및 SASE 플랫폼을 사용하면 ZTNA, CASB, DLP, SWG 정책 간에 컨텍스트가 공유되어 보안 상태가 강화되면서도, 일관된 관리 워크플로우를 통해 구현이 간소화됩니다. 동일한 ID 및 장치 상태 속성으로 ZTNA 및 CASB 액세스 정책과 더불어 SWG 정책에 대한 정보를 모두 알아볼 수 있어 조직 전반의 정책 관리가 간소화됩니다.

ZTNA, 원격 브라우저 격리(RBI), 이메일 보안까지 함께 사용하면 리소스에 조건부 액세스를 제공하면서도 이메일과 협업 도구에서 노출된 악의적 콘텐츠(링크, 첨부 파일)로부터 사용자를 보호할 수 있습니다. 계약자와 사용자가 관리되지 않는 장치를 사용하고 있는 경우에는 데이터 손상을 방지하기 위해 사용자 상호작용(예: 업로드/다운로드, 복사/붙여넣기, 키보드 입력)을 비활성화하여 기업 리소스에 대해 제한적인 액세스를 제공할 수 있고, 기타 L7 DLP 정책을 적용해 중요한 데이터를 감지할 수 있습니다.



고객이 하는 이야기

“Cloudflare Access는 기존 VPN의 훌륭한 대안입니다. 사용자는 소프트웨어를 추가로 다운로드해 구성할 필요 없이, 브라우저를 열고 로그인하기만 하면 됩니다.”

— **Platzi**, 클라우드 엔지니어링 책임자

“Cloudflare Access를 적시에 사용할 수 있게 되어 VPN을 배포하는 번거로움을 겪지 않게 되었습니다. 쉽게 선택할 수 있었고, 놀라울 정도로 배포가 간단했습니다.”

— **ezCater**, 보안 책임자

“내부 자산 액세스를 제한할 때 Access는 VPN보다 훨씬 간단하고 안전합니다. 활성화해서 사용자를 추가하면 됩니다. 그냥 맡겨두면 됩니다!"

— **Bitpanda**, CTO 겸 공동 설립자

"Cloudflare를 이용하기 전에는 안전한 배포를 위해 애플리케이션을 준비하려면 2주~4주쯤 걸리는 프로젝트가 필요했습니다. Cloudflare Zero Trust를 이용하면서 그 시간의 약 90%가 절약되고 있습니다"

— **Creditas**, 네트워크 엔지니어링팀 책임자

분석가의 견해

Cloudflare, 2023 IDC MarketScape for Zero Trust Network Access(ZTNA) 부문에서 리더로 선정

IDC 측은 엔터프라이즈 보안 요구 사항을 지원하는 Cloudflare의 '공격적인 제품 전략'을 리더로 선정된 이유로 듭니다. 우리는 이번 선정으로 모든 규모의 기업에서 Zero Trust를 시작하고 모든 사용자가 VPN 없이 모든 리소스에 안전하게 액세스하도록 지원하는 Cloudflare의 접근 방식이 인정받은 것이라고 생각합니다.

Cloudflare, 2022년 KuppingerCole Leadership Compass ZTNA 부문에서 리더로 선정

KuppingerCole Analysts AG에서는 2022년 ZTNA 시장 분석을 통해 완벽하게 통합되고 유기적으로 개발된 보안 플랫폼, 대규모 글로벌 클라우드 인프라, 대규모 시장 지위와 같은 Cloudflare의 여러 강점을 언급했습니다.

Access 기능

보안 액세스에 제로 트러스트 정책 생성/편집	
상세한 사용자 지정 액세스 정책	중앙화된 정책 관리 경험. 하위 도메인 및 경로 수준에서 와일드카드와 다중 호스트 이름 지원을 통해 L7 앱을 보호하며, CORS 요청을 지원합니다. 몇 초만에 정책 변경 사항을 전역으로 전파합니다. 정책 테스터가 포함되어 있습니다.
폭넓은 리소스: 보호 대상과 보호 방법	리소스는 셀프 호스팅 앱(클라우드/온프레미스) 또는 브라우저 내 SSH/VNC에 대한 역방향 프록시, SaaS 앱에 대한 ID 프록시, 비공개 서브넷 내의 모든 웹 / 비 웹(임시 TCP/UDP) 리소스에 대하여 L4-7 정방향 프록시를 통해 수행되는 클라이언트/터널 기반 비공개 라우팅에 공개 호스트 이름을 사용합니다.
ID	모든 주요 기업 및 소셜 ID 공급자(IdP)를 통해 인증하며 여러 IdP가 동시에 포함됩니다. 일반 SAML과 OIDC 커넥터 역시 사용 가능합니다. 지원 및 강화: 모든 IdP 제공 인증 방법, 임시 인증, 목적 타당성, 전역 또는 앱별 세션에 기반한 재인증 간격, 앱별 또는 사용자별 즉각 세션 취소옵션을 지원하며 강화할 수 있습니다.
장치 상태	장치 클라이언트와 타사 엔드포인트 보호 공급자(EPP) 통합을 사용해 장치 상태를 확인합니다. 서비스간 통합을 사용해 EPP 위험 점수를 제로 트러스트 정책에 가져옵니다.
정책에 대한 컨텍스트 신호	신호(예:이메일 그룹, IP 범위, 지리적 위치, 로그인 방법(예: MFA 유형, IdP 유형), 유효한 mTLS 또는 SSH 인증서, 서비스 토큰, 일련번호 목록, 장치 상태 속성, 설치된 장치 클라이언트, 세션 기간, SWG 규칙 시행, 외부 API 호출의 신호)를 구성합니다. Microsoft Entra ID(Azure AD) 조건부 액세스 정책을 직접 참조할 수도 있습니다.
기타 관련 지원	• **SCIM:** 자체 호스팅 및 SaaS 앱에 사용자를 자동으로 프로비저닝/프로비저닝 해제(예: Okta 및 Azure AD) • **내부 DNS:** 로컬 도메인 폴백 구성 및 비공개 네트워크 요청 해결 • **터널 분할:** 비공개 네트워킹 또는 VPN과 함께 실행 시 IP 포함/제외 • **mTLS 인증:** IoT 및 기타 mTLS 사용 사례에 인증서 기반 인증 • **앱 격리:** 확인란 하나로 번개처럼 빠른 원격 브라우저에 앱 격리*
온램프 및 오프램프	
앱 커넥터	가벼운 앱 커넥터로 간단히 오케스트레이션하면(Cloudflare Tunnel) Cloudflare로 더 빠르게 리소스를 연결할 수 있으며, VM 인프라가 필요하지 않고 처리량 제한이 없습니다. 모니터링, 가상 네트워크(IP 중첩 목적), 이중화 및 장애 조치 기능이 포함됩니다.
장치 클라이언트: 사용 시기	• 클라이언트리스: 관리되지 않는 장치를 사용하는 타사 사용자에게 제로 트러스트 정책을 확장해 적용합니다. 클라이언트리스 RBI 및 L7 DLP 정책과도 잘 작동합니다*. 클라이언트리스 액세스는 웹 앱과 브라우저 내 SSH/VNC를 지원합니다. • 클라이언트 기반: Cloudflare의 장치 클라이언트(Cloudflare WARP)가 비공개 네트워크에 대한 보안 액세스로 확장되어 서비스간 장치 상태 통합이 가능해지며 위치를 인식하여 온프레미스 사용자에게 맞춤형 정책이 적용됩니다. WARP를 실행하는 두 대 이상의 장치를 연결하여 비공개 네트워크를 생성할 수도 있습니다. 사용자가 직접 등록하거나 MDM을 통해 배포할 수 있습니다.
확장성 및 가시성	
페이지 사용자 지정	블록 및 앱 런처 화면에 사용자 지정 HTML을 업로드하여 브랜드에 맞추거나 특정한 액세스 지침을 전달해 최종 사용자 경험을 간소화합니다.
로깅	모든 요청, 사용자, 장치의 로그를 포괄적으로 기록합니다. Logpush나 API를 사용하여 기존 SIEM, 오케스트레이션, 분석 도구와 통합할 수 있습니다. 알려지지 않은 자산의 경우, 내부 인프라용 섀도우 IT가 모든 원점을 드러내는 고유 트래픽을 수동적으로 분류합니다.
자동화	직관적인 API와 Terraform 공급자가 제공되어 모든 Zero Trust 구현 측면을 프로그래밍 방식으로 관리할 수 있습니다. 자동화된 서비스에 유저리스 서비스 토큰 지원도 제공합니다.

**Zero Trust 플랫폼의 다른 부분에 걸쳐 기능 사용*

왜 Cloudflare를 사용해야 할까요?

간편한 설정 및 관리

앱 커넥터 소프트웨어와 터널 오케스트레이션으로 비공개 리소스에 대한 온램프 트래픽 설정과 운영을 과감하게 간소화합니다.

원활한 상시 가동 경험

Cloudflare 글로벌 Anycast 기술을 통해 피크 시의 최종 사용자 성능과 네트워크 중단에 대한 복원력을 확보하여 안정성을 보장합니다.

신속한 얼리어답터 혁신

동종 업계를 선도하며 끊임없이 혁신하는 공급자를 통해 인터넷 자체의 발전을 따라잡고 더 빠르고 안전하게 앱에 액세스합니다.

조직을 위한 간편하면서도 안전한 액세스 알아보기

워크숍 요청하기

CLOUDFLARE

아직 실시간 대화를 할 준비가 되지 않으셨나요?

Cloudflare의 SSE 및 SASE 플랫폼 자세히 알아보기

1. 2023년 설문조사: techvalidate.com/product-research/cloudflare/charts