직원의 생성형 AI 및 에이전틱 AI 사용 보호

Cloudflare SASE 플랫폼에서 제공하는 보호 기능으로 팀이 모든 AI 도구를 안전하게 사용할 수 있도록 지원하세요.

제어력 회복, 생산성 증대

AI 도입 경쟁이 심화되면서 데이터 유출, 규정 위반, 공격면 확대 등 위험이 증가하고 있습니다. AI를 전면적으로 차단하는 것은 경쟁력 약화만 초래하고, 포인트 솔루션을 시험해 보는 것은 복잡성만 가중시킵니다.

Cloudflare는 AI 환경 전반에서 가시성을 확장하고, 위험을 완화하며, 데이터를 전체적으로 보호함으로써 조직의 AI 사용을 안전하게 보호합니다.

- **섀도우 AI를 발견**하고 모든 승인 및 비승인 AI 도구에 대한 정책을 관리하세요.
- ID 기반 액세스 제어 및 상태 관리를 통해 **AI 거버넌스를 강화**하세요.
- 사용자 프롬프트에서 민감한 정보를 차단하고, 주제별 가드레일을 적용하고, AI 도구의 잘못된 구성을 검사하여 **데이터 손실을 방지**하세요.

특정 애플리케이션으로 사용을 제한하는 AI 전략이든, 더 광범위한 다양한 도구를 실험하는 AI 전략이든, Cloudflare를 통해 안전하게 AI를 도입하세요.

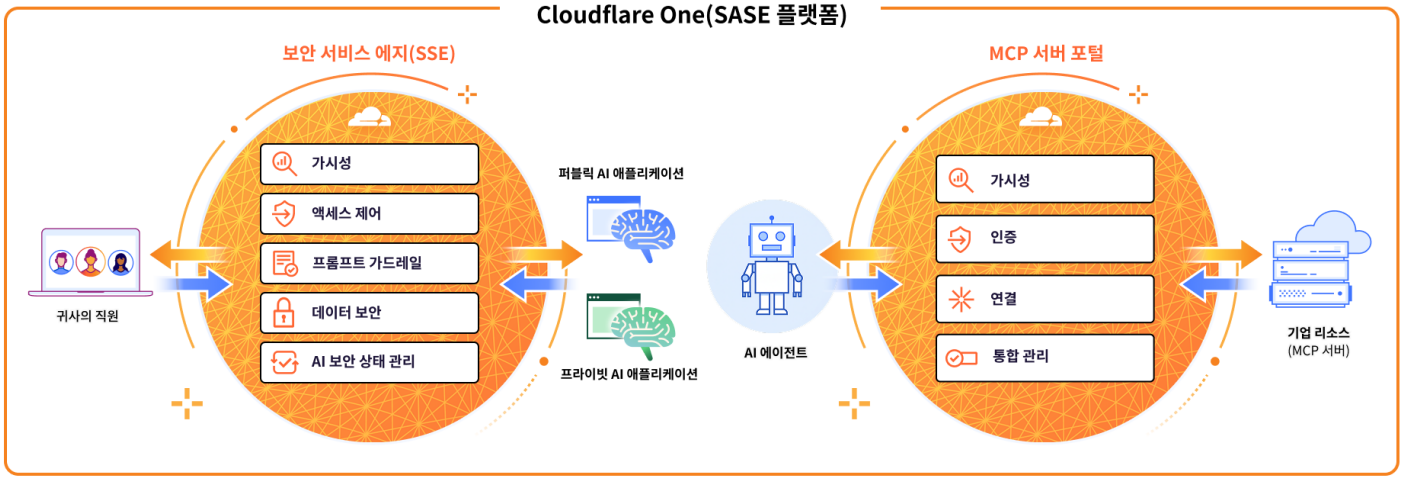
직원의 AI 사용 보호에 SASE가 필요한 이유

Cloudflare의 보안 액세스 서비스 에지(SASE) 플랫폼은 직원과 AI 도구 간의 연결을 중재합니다. 따라서 SASE는 많은 사용자가 AI를 안전하게 시작하는 데 이상적인 출발점입니다.

직원이 ChatGPT와 채팅을 하든, AI 에이전트가 기업 리소스 전반에서 정보를 수집하든, Cloudflare의 SASE 플랫폼은 일관된 보안 제어를 적용합니다.

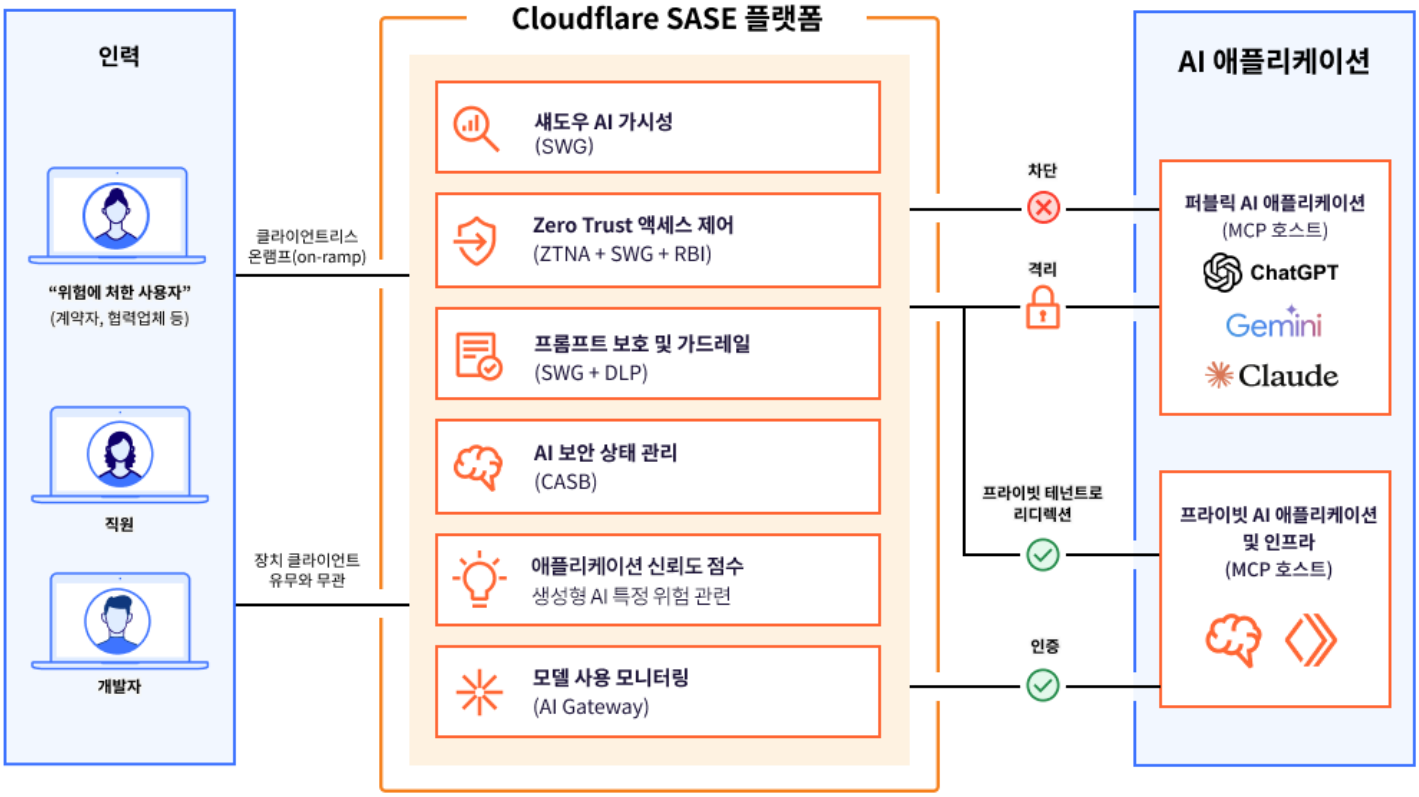
생성형 AI 및 에이전틱 AI 통신 보호

Cloudflare의 SASE 플랫폼은 조직 전체에서 인간-투-AI 및 기계-투-기계 상호 작용을 관리하기 위한 통합 대시보드 및 제어판을 제공합니다.



다른 SASE 벤더와는 달리, Cloudflare는 웹사이트의 AI 챗봇 또는 추천 엔진과 같이 공개적으로 사용 가능한 AI 지원 애플리케이션 및 워크로드를 연결하고 보호하는 데에도 도움을 드립니다.

Cloudflare SASE 플랫폼의 AI 사용 제어 기능으로**생성형 AI 애플리케이션을 사용하는 사용자 통신을 보호**하세요



- **가시성:** 인라인 트래픽 검사를 통해 섀도우 AI 사용을 발견하고 분석합니다. AI 애플리케이션이 초래하는 위험을 투명한 점수로 평가합니다.
- **액세스 제어:** 사용자 연결을 차단, 격리, 리디렉션 또는 허용합니다. 애플리케이션별 ID 기반 Zero Trust 규칙을 적용합니다.
- **프롬프트 보호 및 가드레일:** 사용자 프롬프트를 감지하고 그 의도에 따라 차단합니다(예: 탈옥 시도, 코드 남용, PII 요청).
- **데이터 보안:** PII, 소스 코드 등에 대한 AI 기반 데이터 손실 방지(DLP) 감지 기능으로 중요한 데이터 노출을 방지합니다.
- **AI 보안 상태 관리:** API(ChatGPT, Claude, Google Gemini에서 지금 사용 가능)를 통해 생성형 AI 도구와 통합하고, 클라우드 액세스 보안 브로커(CASB)를 사용하여 잘못된 구성을 검사합니다.

고객 성과

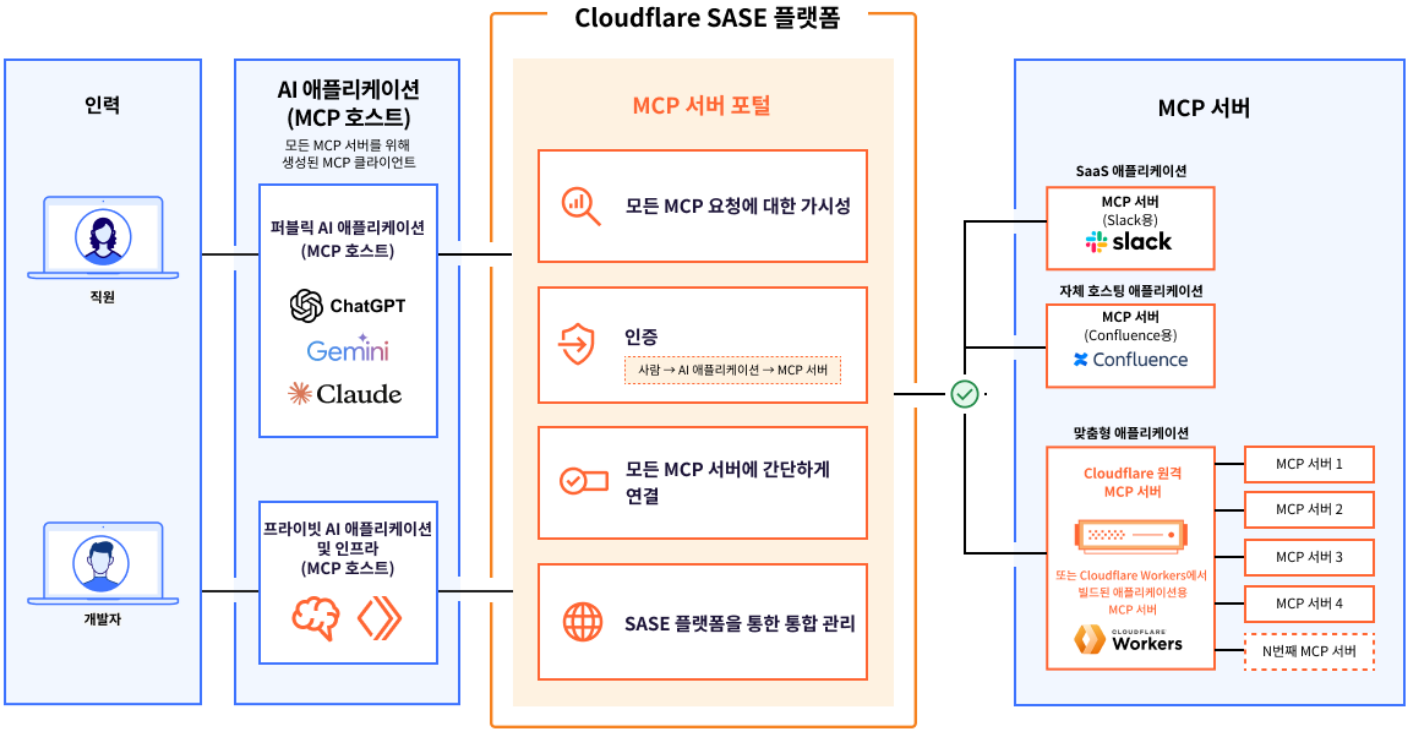
indeed
세계 1위의 구인 웹사이트

VPN 교체 프로젝트와 병행하여 **섀도우 AI를 식별하고 제어**하세요

APPLIED
보험 기술

ChatGPT와 같은 공개 생성형 AI 도구를 격리하여 **중요한 데이터의 복사-붙여넣기를** 차단하세요

Cloudflare SASE 플랫폼에서 MCP 서버 포털을 통해 **에이전틱 AI 통신(AI-투-리소스)을 보호**하세요



- **가시성:** 감사 및 분석을 위해 모든 MCP 요청 로그를 집계합니다. 각 MCP 서버를 검토하고 승인한 후 포털에 추가합니다.
- **인증:** ID를 기반으로 사용자 포털 접근을 인증합니다. 최소 권한 원칙에 따라 MCP 서버에 대한 액세스 범위를 제한합니다.
- **연결:** 각 MCP 서버를 개별적으로 구성하는 대신 단일 URL을 사용하여 액세스 가능한 모든 MCP 서버에 연결합니다.
- **통합 관리:** AI 연결에 대해 인간 사용자와 동일한 세분화된 액세스 정책을 적용합니다.
- **포털별 도구 사용자 지정:** 사용자별로 사용할 수 있는 특정 도구 및 프롬프트 템플릿을 선택합니다.

참고: Cloudflare의 MCP 서버 포털은 Cloudflare에 구축 또는 배포된 모든 원격 MCP 서버를 포함(이에 국한되지 않음)하여 모든 MCP 서버를 지원합니다. 이 기능은 Zero Trust 네트워크 액세스(ZTNA) 제어로 사용할 수 있습니다.

이 블로그에서 Cloudflare의 비전에 대해 자세히 알아보세요.

Cloudflare를 통해 AI를 더욱 안전하게 사용하는 방법을 알아보고 싶으신가요?

워크숍 요청하기

