Cloudflare AI Security Suite

AI 수명 주기 전반에 걸쳐 데이터를 통제하고 위험을 관리하여 AI 상호작용을 보호합니다.

자신 있게 AI 확장

AI 위험에는 최신 보안이 필요합니다.

귀사 팀은 AI를 사용하여 더 빠르게 혁신하고 있지만, 그만큼 중요한 보안 위험을 야기합니다. AI를 차단하거나 복잡한 포인트 솔루션을 추가하는 기존 방식은 혁신을 억누르고 현실을 간과하기 때문에 효과가 없습니다.

- **직원의 85%**가 IT 부서의 검토 전에 AI 도구를 사용합니다.[1]
- **직원의 93%**가 승인 없이 회사 데이터를 AI에 입력했다고 인정합니다.[2]
- **침해된 조직 중 63%**는 AI 거버넌스 정책이 없습니다.[1]

팀의 역량을 강화하고 비즈니스에 필요한 보안과 제어 능력을 유지하는 동시에 AI의 생산성 이점까지 누리는 방법을 알아보세요.

에이전틱 AI 및 생성형 AI 보안을 위한 통합 플랫폼

Cloudflare는 귀사에서 AI를 자신 있게 도입할 수 있도록 단일 플랫폼을 제공합니다. Cloudflare는 보안 책임자가 위험을 관리하고, 기술팀이 생산성을 높이며, 플랫폼 엔지니어가 안전하게 빌드할 수 있도록 지원함으로써 모든 사람이 안전하게 함께 혁신할 수 있도록 지원합니다.

Cloudflare AI Security Suite 시작하기

Cloudflare AI Security Suite는 AI 도구의 작업 공간 사용 및 퍼블릭 애플리케이션 보안을 위한 통합 플랫폼에서 제공됩니다. 섀도우 AI를 식별하고, 모델이 오용되지 않도록 보호하며, 에이전트 액세스를 안전하게 유지하고, 프롬프트에서 데이터가 노출되지 않도록 방지하여 기업이 더 쉬운 가시성과 강력한 제어 기능을 통해 안전하고 효율적으로 혁신할 수 있도록 도와줍니다.

가시성 확장

AI 애플리케이션, API 엔드포인트, AI 에이전트 연결 전반에 걸친 확장

위험 완화

가드레일, 상태 제어, 실시간 위협 완화 활용

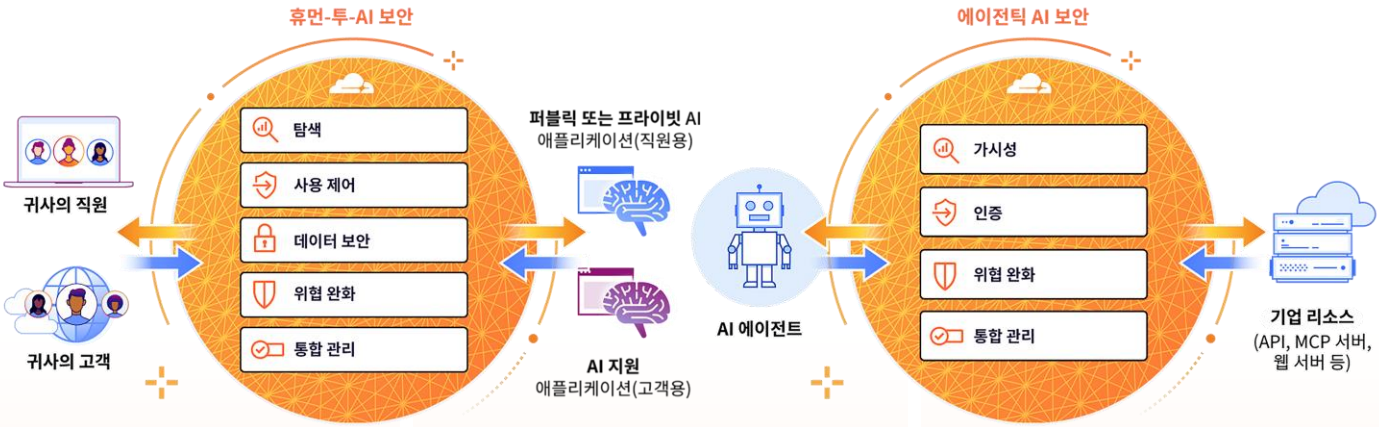
데이터 보호

직원 및 AI 에이전트에 대한 신속한 보호 및 액세스 제어

Cloudflare에서 AI를 개발하면 보안이 기본 내장됩니다.

Cloudflare AI 보안 제품군으로 생성형 및 에이전트 AI 통신 보호

생성형 AI에서 인력이 사용하는 데이터를 제어하고, 자율 에이전트가 야기하는 보안 위험을 관리하여 모든 AI 통신을 보호하세요.

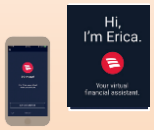


- **인력:** 직원, 계약업체, 개발자 등
- **귀사 고객:** 웹사이트 및 애플리케이션 방문객

- **생성형 AI 애플리케이션:** 독립형 또는 임베디드

Gemini Claude ChatGPT Copilot

- **AI 기반 애플리케이션** 예: Bank of America의 AI 챗봇, Erica



- **API** 및 **MCP 서버**(모든 애플리케이션용)

Google Workspace

- 추론 및 검색 증강 생성(RAG)을 위한 **웹 서버**

AI 수명 주기 전반에 걸쳐 설계형 보안을 통해 AI 채택 가속화

직원들의 AI 사용 보호

AI 사용 제어 및 AI 보안 상태 관리(AI-SPM)를 구현하여 위험을 완화하고 데이터를 보호합니다.

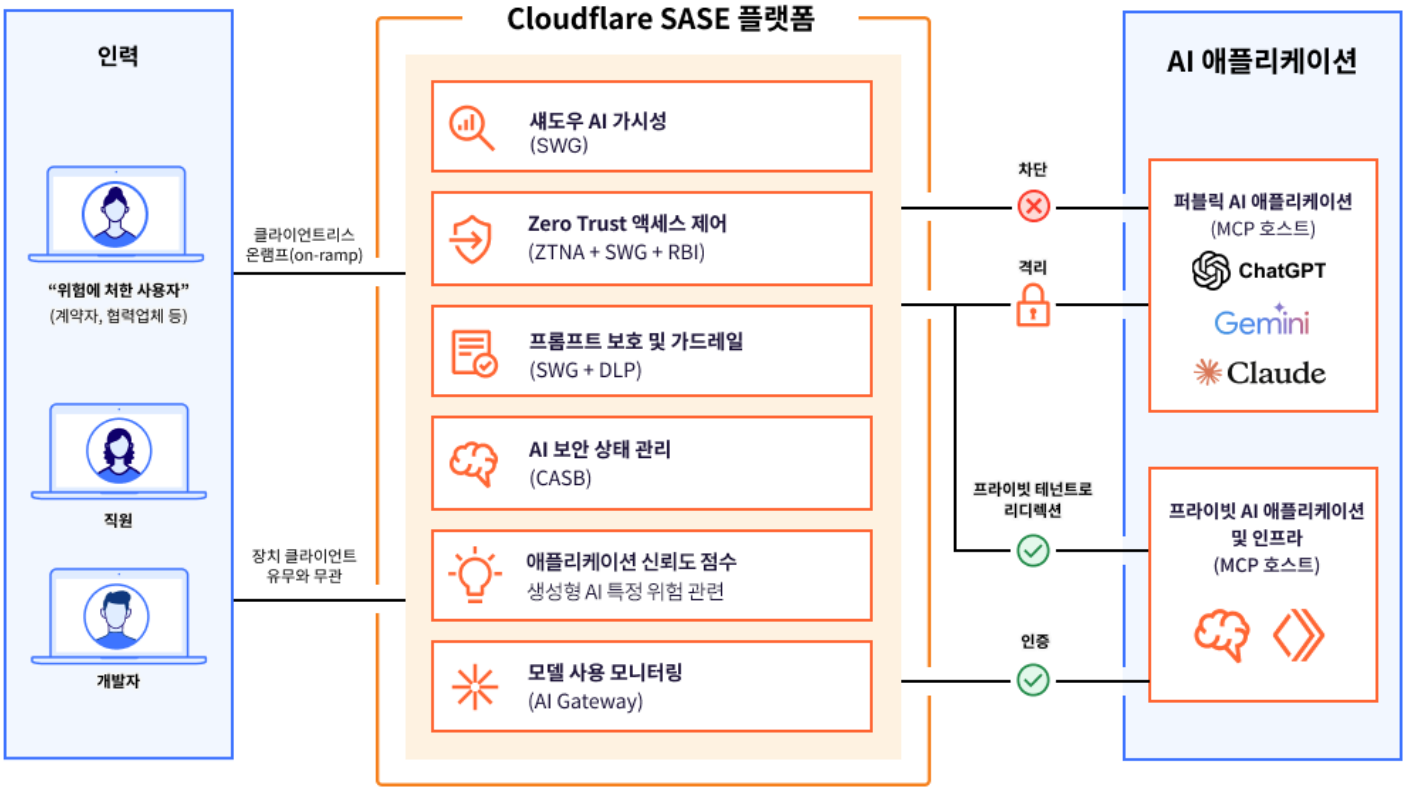
AI 기반 애플리케이션 보호

AI 애플리케이션과 API를 프롬프트 삽입 및 데이터 유출로부터 실시간 보호하세요.

안전한 AI 구축

통합되어 있는 관찰 가능성, 레이트 리미팅, 인라인 AI 가드레일을 통해 개발자가 AI 애플리케이션을 보호하도록 지원하세요.

Cloudflare의 SASE 플랫폼을 통해 직원의 AI 애플리케이션 사용 및 워크로드를 안전하게 보호



SSE를 통해 인간-투-AI 통신 보호

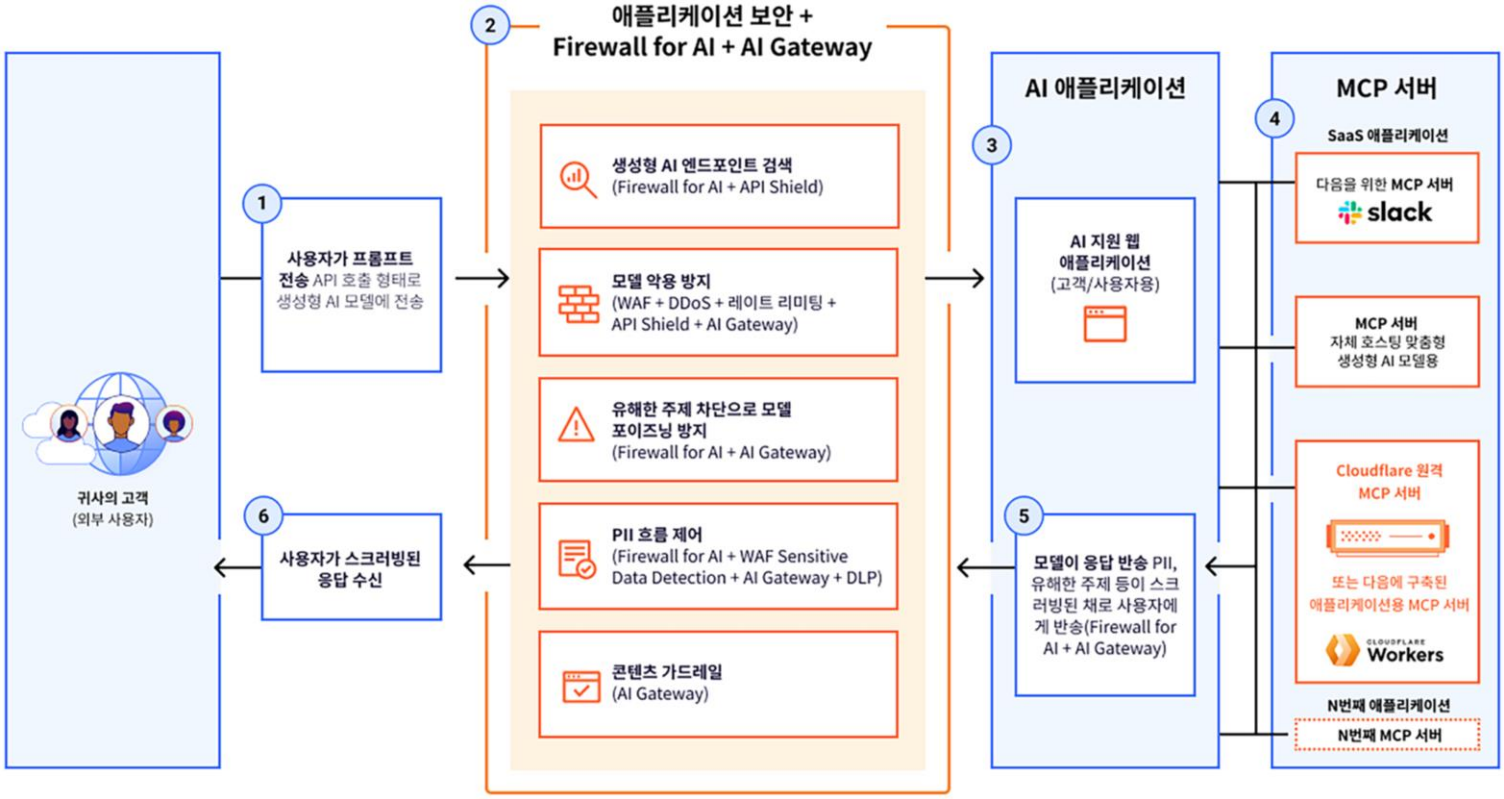
- **가시성:** 인라인 트래픽 검사를 통해 섀도우 AI 사용을 발견하고 분석합니다. AI 애플리케이션이 초래하는 위험을 투명한 점수로 평가합니다.
- **액세스 제어:** 사용자 연결을 차단, 격리, 리디렉션 또는 허용합니다. 애플리케이션별 ID 기반 Zero Trust 규칙을 적용합니다.
- **프롬프트 보호 및 가드레일:** 의도에 따라 사용자 프롬프트를 감지하고 차단합니다(예: 탈옥 시도, 코드 남용, PII 요청).
- **데이터 보안:** PII, 소스 코드 등에 대한 AI 기반 데이터 손실 방지(DLP) 감지 기능으로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

AI-투-리소스 통신 보호를 위한 MCP 서버 포털

- **가시성:** 감사 및 분석을 위해 모든 모델 컨텍스트 프로토콜(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 사람 사용자와 동일한 세분화된 액세스 정책을 적용합니다.

참고: MCP 서버 포털은 Cloudflare에서 구축하거나 배포하는 원격 MCP 서버를 포함하여 모든 MCP 서버를 지원합니다. 이 기능은 Zero Trust 네트워크 액세스(ZTNA) 제어로 사용할 수 있습니다.

Cloudflare의 모델 독립적인 인라인 보안으로 AI 기반 애플리케이션과 워크로드 보호



다음 기능을 갖춘 애플리케이션 보안 및 Firewall for AI로 공개 AI 보호

- **생성형 AI 엔드포인트 검색:** 웹 자산 전반에서 모든 AI 모델과 API를 자동으로 검색합니다.
- **AI 모델을 악용으로부터 보호:** 맞춤형 Firewall for AI를 사용하여 프롬프트 삽입, 모델 포이즈닝, 과도한 사용 및 기존 보안 기능을 우회할 수 있는 기타 위협을 차단합니다.
- **PII 흐름 제어:** 사용자 프롬프트 및 모델 응답을 스캔하여 중요 데이터가 노출되지 않도록 차단함으로써 규제 준수를 지원합니다.
- **콘텐츠 가드레일:** Llama Guard와 같은 통합 모델을 사용하여 안전하지 않거나 유해한 프롬프트를 차단합니다. 사용자 지정 WAF 규칙을 생성하여 의심스러운 AI 상호 작용을 쉽게 차단하거나 기록합니다.

개발자 플랫폼 및 AI Gateway로 빌드하는 AI 보호

- **통합 AI 제어판:** 단일 대시보드에서 모든 AI 애플리케이션을 관리합니다. 요청 라우팅, 응답 캐시, 비용 관리 및 성능 모니터링을 수행합니다.
- **에지에서 자격 증명 보호:** 에지에서 API 키와 보안 정보를 안전하게 저장하여 클라이언트 측 노출을 막고 공급자 전반에서 키 교체를 간소화합니다.
- **콘텐츠 안전 가드레일 적용:** 프롬프트와 응답에서 유해 콘텐츠 및 개인 식별 정보를 자동으로 식별, 차단 또는 수정합니다.

Cloudflare는 귀사의 퍼블릭 및 프라이빗 AI 환경을 모두 보호하는 유일한 공급업체입니다.

AI에 적합한 가드레일을 구현하여 자신 있게 AI를 도입하고, 혁신을 저해하지 않는 보안을 통해 혁신을 가속화하세요.

- **통합 AI 생태계 보호:** 복잡한 보안 스택은 위험을 증가시킵니다. 단일 플랫폼으로 데이터를 보호하고 AI 수명 주기 전반에서 규제 준수를 보장하세요.
- **미래 보장형 글로벌 아키텍처:** 모든 트래픽 볼륨에 맞춰 확장 가능하고, 새로운 위협에 지속적으로 적응하며, 새로운 사용 사례에 프로그래밍할 수 있는 포스트 퀀텀 보안 네트워크를 통해 미래의 문제를 오늘 바로 예방하세요.
- **AI 기반 보안:** Cloudflare의 AI 기반 방어 시스템은 프롬프트와 응답을 검사하여 실시간 위협을 감지합니다.
- **검증된 AI 리더십:** 상위 50대 생성형 AI 기업의 80%가 신뢰하는 플랫폼에서 자신감을 가지고 혁신하세요.
- **모델에 구애받지 않는 배포:** 보안 제어는 귀사 환경의 모든 AI 모델에 대해 작동하면서 AI 배포를 관리하는 단일 통합 접근 방식을 제공합니다.

고객이 하는 이야기

indeed

세계 1위의 구인 웹사이트
사례 연구 보기

섀도우 AI 식별 및 제어

VPN 교체 프로젝트와 병행

APPLIED

보험 기술
사례 연구 보기

ChatGPT와 같은 공개 생성형 AI 도구 격리

중요 데이터 복사-붙여넣기 차단

AI 기반 SaaS 기업

개인 식별 정보 보호

고객이 공개 생성형 AI 엔드포인트에 중요한 정보를 제출하는 것을 방지

Cyndx

AI 기반 핀테크

추론 비용 95% 절감

Cloudflare를 채택하여 AI 모델 공급자의 응답을 캐시하고 실행

AI 보안 니즈에 관해 상담할 준비가 되셨나요?

전문가 상담

1. 2025 Manage Engine 연구: 출처
2. 2025 IBM, 데이터 유출 비용 보고서: 출처

 | 007-9814-2030-192 | enterprise@cloudflare.com | www.cloudflare.com/ko-kr/