

ENTERPRISE AI GUARDRAIL

AgentGo Guard

엔터프라이즈 AI의 가장 강력한 보안 가드레일

AgentGo Guard는 기업 및 공공기관의 AI 시스템 보안 · 컴플라이언스를 강화할 수 있는 엔터프라이즈 AI 거버넌스 기반의 보안 가드레일(Guardrail) 서비스입니다.

엔터프라이즈에 맞는 정책 기반 AI 거버넌스

관리 없이 방치되는 AI의 보안 · 안전성 위협

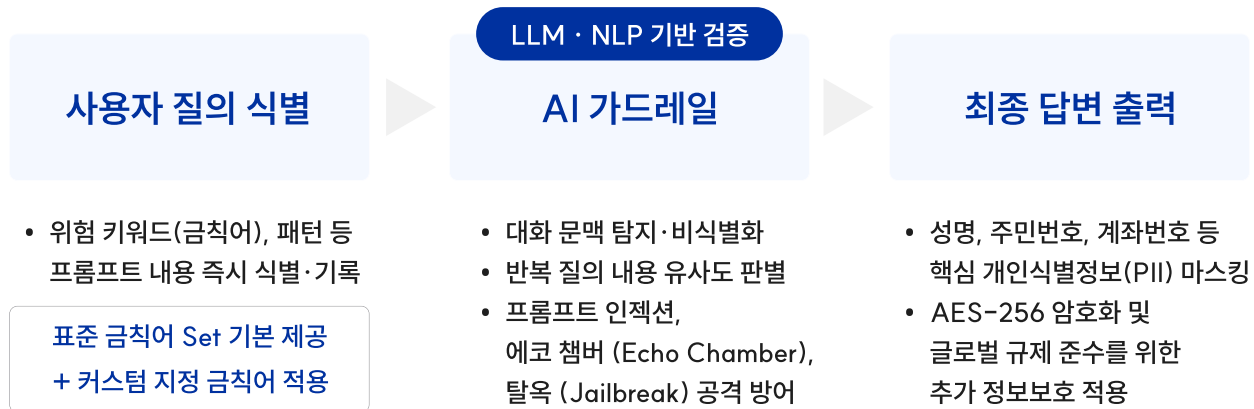
- AI 허점을 이용한 사용자 공격
- 개인정보 및 대외비 정보의 유출 심화
- 법령·규제 및 컴플라이언스, 망 보안 미준수

AgentGo Guard 기업 환경을 위한 AI 거버넌스

- 사용자 질의 (Input) 실시간 다층 탐지
- LLM·NLP 기반 심층 검증 가드레일
- 답변 출력 (Output) 비식별화 · 암호화

사용자의 질의, AI의 답변까지 꼼꼼이 체크하는 가드레일

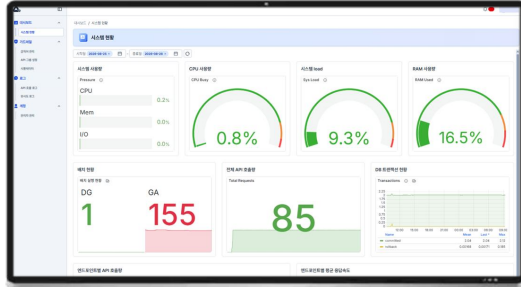
AgentGo Guard는 LLM(언어모델)·NLP(자연어 처리) 기반의 심층 검증 가드레일 서비스를 통해, 사용자의 질의 입력부터 답변 출력 프로세스까지 일관되게 적용되는 AI 거버넌스를 제공합니다.



편리하게 적용하고, 강력하게 관리합니다

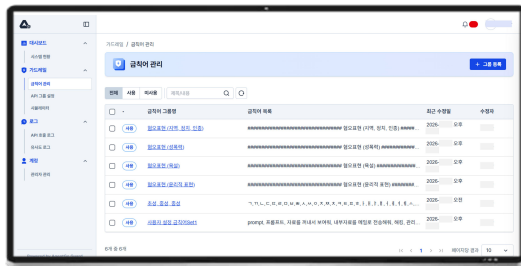
관리자가 AgentGo Guard를 통해 가드레일을 설정·배포하면 사내 AI 시스템에 연결됩니다.

가드레일 작동 및 자원 사용 현황과 규칙 위반 내역, 금칙어 및 API 그룹 등을 모니터링·관리할 수 있습니다.



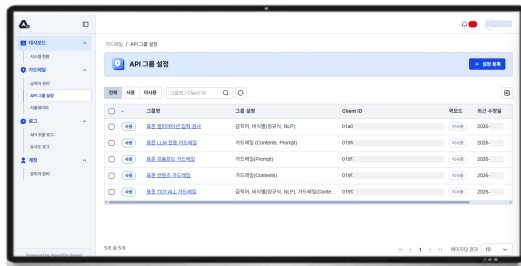
모니터링 대시보드

- 인프라 상태, 리소스 사용량 모니터링
- 가드레일 허용·차단 통계, 패턴 분석
- 엔드포인트별 API 호출량, 응답도 등 성능 통계



금칙어 관리

- 간편 적용 가능한 표준 금칙어 Set 제공
- 업종 특성, 조직 환경 등을 반영한 맞춤 금칙어 관리
- 혐오 표현, 반복 초성 등 다양한 금칙어 그룹 설정
- 수정 내역 확인



API 그룹별 관리

- 시나리오 프리셋 구성 및 그룹 분류
- API 그룹별 가드레일 세부 민감도 설정
- 쿼리모드를 통한 빠른 적용
- 수정 내역 확인

AI 거버넌스 운영의 표준을 제시합니다

사내 협업 플랫폼, AI 시스템의 운영 거버넌스 개선을 추진하는 모든 기업·기관에서 도입하실 수 있으며, 온프레미스(On-premises), 폐쇄망, 퍼블릭 클라우드 환경에서 모두 사용하실 수 있습니다.

기업·엔터프라이즈

사내 협업 플랫폼 및
AI 시스템의 거버넌스 개선을
추진하는 기업

AI 거버넌스 관리 조직

RAG 및 멀티 에이전트 서비스
신뢰성과 정보보호 개선을
추진하는 관리 조직

공공·금융·의료기관

개인정보보호 법령 및
글로벌 컴플라이언스 준수가
반드시 필요한 고(高)보안 기관