SOVEREIGN AI CONTROL PLANE

AI KEEPER

SECURING AI PLATFORM

기업 AI 운영을 위한 통합 거버넌스 플랫폼

기업 내 LLM과 AI 서비스를 하나의 Self-Hosted Gateway로 통합하여
보안, 정책, 감사 체계를 일관되게 적용하는 AI Governance 플랫폼

Unified Governance

Self-Hosted & Air-Gap

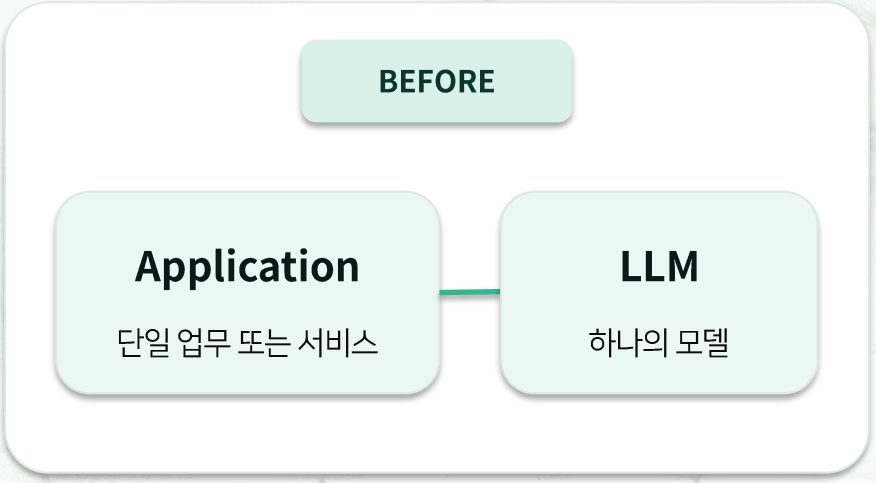
Compliance Ready

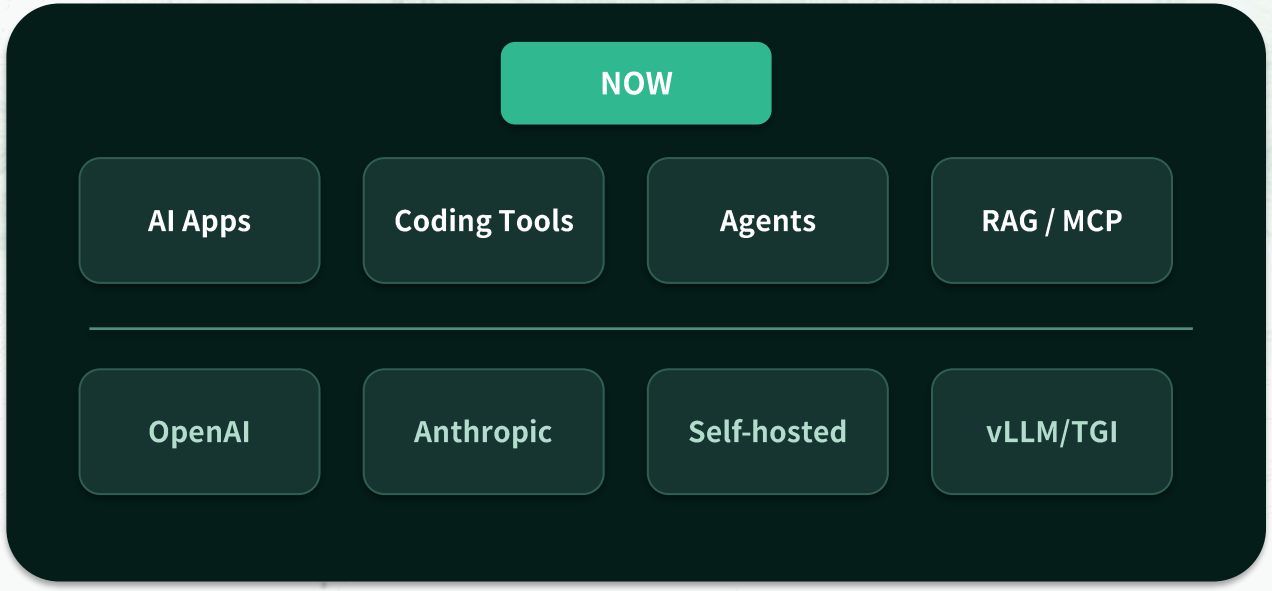
Seamless Integration

WHY 02. Enterprise AI 환경의 변화

하나의 AI를 쓰던 환경에서, 여러 AI가 함께 작동하는 환경으로

상용 LLM, 자체 구축 모델, AI Coding Tool, RAG, MCP, AI Agent가 **하나의 조직 안에서 동시에 사용**됩니다.





WHY 03. Fragmented AI Governance

AI 활용의 확장은 곧 관리 대상의 확장을 의미합니다.

AI 서비스가 **개별적으로 도입**되면서 정책, 인증 정보, 사용 이력, 비용 관리가 **따로 운영**되기 시작합니다.

Security Policy

부서·서비스마다 다른 Guardrails와 보안 정책

API Key

개발자 및 애플리케이션별 인증 정보 분산

Audit Log

모델·서비스별로 흩어진 요청 및 정책 적용 이력

Token & Cost

팀·프로젝트별 사용량과 비용에 대한 제한된 가시성

WHY 04. 왜 기존 방식으로 관리하기 어려운가

AI마다 보안을 추가하는 방식으로는 통합 거버넌스를 만들기 어렵습니다.

AI 서비스별 개별 관리

- 모델마다 별도의 정책 설정
- API Key 및 권한 개별 관리
- 로그 저장 위치와 형식 분산
- 보안 · 감사 솔루션 추가 연동

관리 대상이 증가할수록

운영 복잡성 ↑

정책 불일치 ↑

통합 가시성 ↓

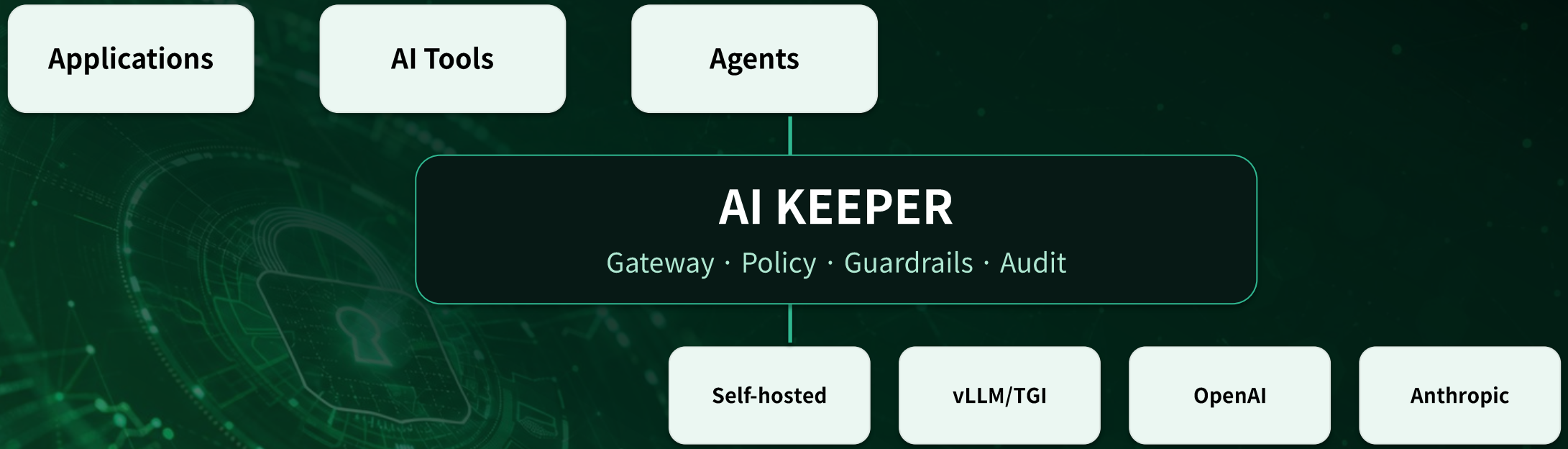
필요한 것은 AI를 관리하는 기준을 하나로 만드는 것입니다.

HOW

05. AI Keeper: Router of Routers

분산된 AI 환경에 하나의 Control Layer를 만듭니다.

각 서비스에 개별 통제 기능을 구축하는 대신, AI 요청이 통과하는 중앙 지점에서
Routing · Security · Policy · Audit · Usage Control을 일관되게 적용합니다.



HOW

06. Architecture

AI 트래픽 전반을 하나의 정책 체계 (Gateway) 아래 관리합니다.

① AI Applications & Request	CodeCenter · AI Coding Tool · RAG/MCP · Agent · Custom App
② AI Keeper Control Layer	Authentication → Guardrails → Policy → Routing → Audit / Usage
③ LLM Router & Model	Self-hosted LLM · vLLM/TGI · OpenAI · Anthropic

WHAT 07. Security & Policy

모든 AI 요청에 동일한 보안 기준을 적용합니다.

AI 서비스마다 개별적으로 보안 기능을 구성하는 것이 아닌, AI Keeper에서 정의한 정책을 요청 단계에서 일관되게 적용합니다.

1 Single Enforcement Point

모델과 애플리케이션에 관계없이 중앙 정책 적용

2 Prompt & Data Protection

Prompt Injection 및 PII 등 요청·응답 과정의 위험 통제

3 Centralized Guardrails

보안 정책을 중앙에서 관리하고 일관되게 적용

WHAT

08. Control & Governance

누가, 어떤 AI를, 얼마나 사용할 것인지 관리합니다.

사용자·팀·프로젝트 단위로 AI 이용 기준을 설정하고, 인증 정보와 사용량을 하나의 운영 정책으로 연결합니다.

1 API Key Centralization

개인별 외부 API Key 사용을
차단하고 인증 정보를 중앙 관리

2 Multi-Tenancy

팀·프로젝트·사용자별
AI 환경과 정책 분리

3 Quota & Token Budget

사용량과 Token Budget을
기준으로 AI 이용 범위 제어

WHAT

09. Observability & Audit

AI가 어떻게 사용됐는지 추적 가능한 기록으로 남깁니다.

정책 적용 여부뿐 아니라 실제로 **어떤 요청이 발생했고 어떤 기준이 적용됐는지** 확인할 수 있는 운영 가시성을 제공합니다.

1 Complete Audit Trail

AI 요청·응답과 정책 적용 이력을 기록

2 Usage Visibility

사용자·팀·프로젝트별 AI 및 Token 사용량 파악

3 OpenTelemetry Native

표준 Telemetry 기반 Tracing 및 Metrics 연동

WHAT

10. MCP & Agent Governance

AI Agent가 사용하는 Tool까지 거버넌스 범위를 확장합니다.

Agentic AI 환경에서는 Agent가 어떤 **MCP Server와 Tool에 접근하고 무엇을 실행할 수 있는지**도 새로운 통제 영역이 됩니다.

1 Private MCP Registry

조직에서 허용한
MCP Server 관리

2 Access Control

RBAC 기반 사용자 · Agent
Tool 접근 권한 제어

3 Authentication

Per-user OAuth 및
기업 IdP 연계

4 Sandboxing

Tool 실행 영역과 권한을
제한하여 실행 위험 관리

PROOF 11. Enterprise Compliance

규제별 핵심 요구사항을 실제 운영 기능과 연결합니다.

규제·표준	주요 요구사항	AI Keeper 대응
EU AI Act	Article 9~14: 리스크 관리, 데이터 거버넌스, 기술 문서화, 6개월 로그 보관, 인간 감독	Self-hosted 환경에서 감사 로그 자체 보관, AIBOM 자동 생성, 실시간 정책 강제, 구조화된 규제 증거 축적
NIST AI RMF	Govern / Map / Measure / Manage 4대 기능	Control-to-Requirement 매핑 테이블 공개, 각 기능별 시스템 레벨 강제
ISO/IEC 42001	AI 관리 시스템 인증	정책 강제, 자산 인벤토리, 지속적 모니터링, 감사 추적
OWASP	LLM01~LLM10 전체 취약점 대응	Prompt Injection(LLM01) 등 시스템 레벨 방어, 각 결정 구조화 로그 기록

정책 적용 → 운영 → 기록 → 감사까지 하나의 Governance Layer에서 연결

PROOF

12. Operational Value

여러 솔루션을 개별 운영하는 복잡성을 줄이고

하나의 Governance Layer에서 통제와 가시성을 확보합니다.

<200ms

Governance Latency

정책·Guardrails 처리 추가 지연

4x+

Lower TCO

개별 Point Solution 구성 대비

100%

OWASP Agentic AI Coverage

정의된 평가 항목 기준

ZERO

Ungoverned AI Requests

AI Keeper 관리 범위 기준

ADOPTION

13. Deployment Architecture

데이터와 정책을 기업의 통제 범위 안에서 운영합니다.

조직의 인프라와 보안 정책에 따라 다양한 형태로 AI Keeper를 구축할 수 있습니다.

On-Premises

AI 데이터와 거버넌스 환경을 내부 인프라에서 직접 운영

Air-Gapped

외부 네트워크 연결이 제한된 폐쇄망 환경에서 독립 운영

Hybrid

내부 인프라와 외부 서비스를 하나의 거버넌스 Layer에서 관리

Azure GovCloud

공공·규제 환경을 위한 전용 클라우드 구축 옵션

분산된 AI 운영을 하나의 거버넌스 체계로

기존 AI 환경은 유지하면서, AI를 운영하는 기준을 하나로 통합합니다.

BEFORE

AI 서비스별 개별 운영

</>	CodeCenter Claude Code	→	OpenAI · Anthropic Self-hosted LLM
DB	RAG / MCP AI Agent	→	자체 LLM · vLLM/TGI
APP	Custom AI Application	→	외부 API · 내부 모델

정책 · API Key · 로그 · 사용량을 서비스별로 개별 관리
보안 정책 불일치 · 가시성 부족 · 비용 통제 한계

AI Keeper

하나의 Governance Layer

Security · Policy · Access · Audit · Control

AFTER

하나의 기준으로 통합 관리

공통 보안 정책
모든 AI 요청에 동일한 Guardrails 적용

중앙 권한 관리
사용자 · 팀별 AI 접근 정책 통제

통합 가시성
AI 요청 · 사용량 · 비용을 한 곳에서 추적

Audit Trail
AI 사용 및 정책 적용 이력을 중앙 기록

AI KEEPER 도입 효과

보안·정책 일관성
모든 AI 서비스에 동일 기준

운영 효율성
개별 관리 복잡성 감소

비용 가시성
사용량·비용 통합 추적

감사 대응
통합 이력 기반 추적

AI KEEPER

우리 조직의 AI 환경에도
하나의 통제 기준이 필요합니다.

AI Keeper는 기존 AI 환경을 기반으로
보안·정책·권한·감사·사용량을 하나의 Governance Layer로 통합합니다.

PoC 협의

One Gateway. Complete Control.

www.slexn.com

AI KEEPER
SECURING AI PLATFORM

SLEXN
IT Solution & Service Provider