THAKI Cloud



Enterprise Agent Platform

Paxis

Contents

1. Overview 02

2. Paxis 04

3. 비즈니스 임팩트 06

4. Paxis 제품 구성 08

- Agent Builder
- Enterprise RAG Engine
- MCP Tool Hub
- Chat Interface
- Endpoint Account

5. Enterprise Agent 운영 과제 및 Use Cases 14

Appendix: High-Level Architecture 16

1. Overview

엔터프라이즈 에이전트 플랫폼, 방화벽 내부에서 AI 에이전트 워크플로우를 구축하고 운영합니다.

엔터프라이즈 에이전트 플랫폼은 기업 내부 데이터와 업무 시스템을 기반으로 온프레미스 환경에서 에이전트를 설계, 실행, 관리할 수 있도록 지원합니다. 에이전트 빌더로 업무 흐름을 구성하고 RAG와 MCP Tool Hub로 내부 지식과 시스템을 연결할 수 있습니다. 또한 AI training/inference 플랫폼에서 생성한 모델 엔드포인트로 에이전트를 실행 환경에 연계할 수 있습니다.

01 방화벽 내부 에이전트 운영

엔터프라이즈 에이전트 플랫폼은 민감한 기업 데이터와 에이전트 실행 환경을 방화벽 내부에서 운영할 수 있도록 지원합니다. 외부 시스템 의존을 줄이고, 조직의 보안 정책과 규제 요건에 맞는 에이전트 운영 체계를 구성할 수 있습니다.

02 내부 데이터 기반 응답 정확도

Enterprise RAG Engine은 내부 문서, 정책, 데이터베이스를 에이전트가 활용할 수 있는 신뢰 가능한 지식 기반으로 연결합니다. 하이브리드 검색과 문서 처리 파이프라인을 통해 도메인 특화 질의에 더 정확하고 근거 있는 응답을 제공합니다.

03 에이전트 구축 및 시스템 연계

엔터프라이즈 에이전트 플랫폼은 노코드 기반 Agent Builder로 업무 흐름을 설계하고, MCP Tool Hub를 통해 ERP, CRM, ITSM 등 사내 시스템과 에이전트를 연결합니다. 또한 AI inference 앱에서 생성한 모델 Endpoint를 에이전트에 연계하여 기업 맞춤형 모델 기반의 에이전트 워크플로우를 구성할 수 있습니다.

THAKI Cloud

2. Paxis

기업 AI 에이전트는 내부 데이터와 업무 시스템 안에서 안전하게 운영되어야 합니다.

방화벽 내부 실행, Enterprise RAG, MCP 기반 시스템 연계, Endpoint 연동을 통해 기업 환경에 적합한 에이전트 운영 체계를 제공합니다.

AI 에이전트가 실제 업무를 수행하려면 단순한 대화 기능을 넘어 내부 데이터, 업무 시스템, 보안 정책과 긴밀하게 연결되어야 합니다. 그러나 외부 API와 클라우드 중심의 에이전트 운영 방식은 민감 데이터 통제, 규제 준수, 시스템 연계 측면에서 한계를 가질 수 있습니다.
엔터프라이즈 에이전트 플랫폼은 기업이 승인한 인프라와 데이터 환경 안에서 에이전트를 구축하고 운영할 수 있도록 지원합니다.

01 방화벽 내부 에이전트 운영

엔터프라이즈 에이전트 플랫폼은 민감한 기업 데이터와 에이전트 실행 환경을 방화벽 내부에서 운영할 수 있도록 지원합니다. 외부 API 의존과 데이터 노출 리스크를 줄이고, 조직의 보안 정책과 규제 요건에 맞는 에이전트 운영 체계를 제공합니다.

02 외부 API 의존과 운영 비용 통제

엔터프라이즈 에이전트 플랫폼은 에이전트 실행 환경을 기업 내부 인프라와 승인된 모델 Endpoint 중심으로 구성할 수 있도록 지원합니다. 외부 LLM API 의존도를 낮추고, 종량제 비용과 벤더 종속 리스크를 줄여 예측 가능한 에이전트 운영 체계를 확보할 수 있습니다.

03 사내 시스템과의 안전한 연계

MCP Tool Hub는 ERP, CRM, ITSM 등 기업의 기존 업무 시스템과 에이전트를 연결합니다. 인증, 실행 로그, 도구 호출 추적을 기반으로 에이전트가 내부 시스템과 안전하게 상호작용할 수 있도록 지원합니다.

04 노코드 Agent Builder

엔터프라이즈 에이전트 플랫폼은 복잡한 에이전트 워크플로우를 코드 작성 없이 설계할 수 있는 노코드 빌더를 제공합니다. 사용자는 업무 단계, 도구 호출, 데이터 조회, 응답 흐름을 쉽게 구성하며 기업 내부 시스템과 연결된 에이전트를 빠르게 운영 환경에 적용할 수 있습니다.

3.
비즈니스 임팩트

엔터프라이즈 에이전트 플랫폼은 에이전트 도입을 실험 단계에서 실제 사내 업무 성과로 전환합니다.

내부 데이터 기반 자동화, 온프레미스 운영, 사내 시스템 연계를 통해 업무 처리 속도, 운영 비용, 보안 통제 측면의 실질적인 비즈니스 효과를 제공합니다.

AI 에이전트의 가치는 단순한 대화 기능이 아니라, 기업의 실제 업무 흐름 안에서 반복 업무를 줄이고 신뢰 가능한 의사결정을 지원할 때 발생합니다. 엔터프라이즈 에이전트 플랫폼은 노코드 Agent Builder, Enterprise RAG Engine, MCP Tool Hub, AI inference 앱의 Endpoint 연계를 통해 에이전트를 더 빠르게 구축하고, 더 안전하게 운영하며, 더 넓은 업무 영역으로 확장할 수 있도록 지원합니다.

01 에이전트 구축 리드타임 단축

엔터프라이즈 에이전트 플랫폼은 노코드 Agent Builder에서 에이전트가 쓸 모델·스킬·도구와 연결할 사내 시스템을 고르고, 구성을 한눈에 확인할 수 있도록 지원합니다. 개발 리소스 의존도를 낮추고, 현업 요구사항을 더 빠르게 에이전트 워크플로우로 전환할 수 있습니다.

02 업무 자동화 범위 확장

엔터프라이즈 에이전트 플랫폼은 문서 검색, 정책 검토, 고객 응대, 보고서 초안 작성, 시스템 조회와 같은 반복 업무를 에이전트 기반 워크플로우로 전환합니다. 이를 통해 업무 처리 시간을 줄이고, 직원이 더 높은 가치의 판단과 실행에 집중할 수 있도록 지원합니다.

03 외부 API 비용 및 벤더 종속 완화

엔터프라이즈 에이전트 플랫폼은 기업 내부 인프라와 승인된 모델 Endpoint 중심으로 에이전트 실행 환경을 구성할 수 있도록 지원합니다. 외부 LLM API 호출 의존도를 낮추고, 종량제 비용과 벤더 종속 리스크를 줄여 장기적인 운영 비용을 더 예측 가능하게 만듭니다.

04 현업 생산성과 IT 운영 효율 향상

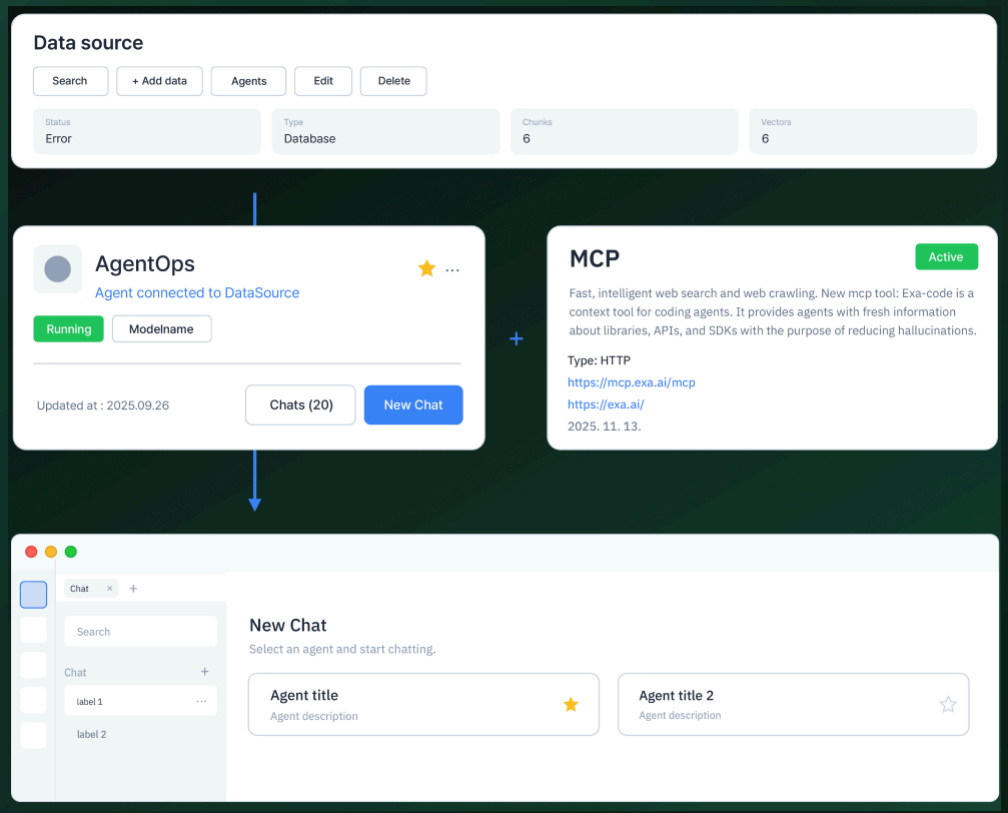
현업 조직은 코드 작성 없이 업무 자동화 시나리오를 설계하고, IT 조직은 보안 정책, 시스템 연계, 실행 환경을 표준화해 관리할 수 있습니다. 엔터프라이즈 에이전트 플랫폼은 기업 조직 전반에서 운영 가능한 AI 역량으로 확장 가능하도록 완성도 높은 운영 환경을 제공합니다.

THAKI Cloud

4.
Paxis 제품 구성

Agent Builder : 코드 없이 에이전트 워크플로우를 설계하는 노코드 빌더

Agent Builder는 복잡한 개발 과정 없이 에이전트를 생성하고, 사전에 구성된 MCP Tool과 데이터 소스를 연결할 수 있는 노코드 구성 환경입니다. 사용자는 에이전트의 역할, 시스템 프롬프트, 참조할 데이터, 실행할 도구를 간단히 설정해 기업 업무에 맞는 에이전트를 빠르게 구성할 수 있습니다.



에이전트 생성 및 설정

업무 목적에 맞는 에이전트를 생성하고, 이름, 설명, 역할, 실행 지침을 손쉽게 설정합니다.

MCP Tool 연결

사전에 생성한 MCP Tool을 에이전트에 연결해 사내 시스템 조회, 업무 실행, 외부 도구 호출을 수행할 수 있습니다.

데이터 소스 연결

문서, 정책, 데이터베이스 등 등록된 데이터 소스를 에이전트에 연결해 내부 지식 기반 응답을 구성합니다.

프롬프트 커스터마이징

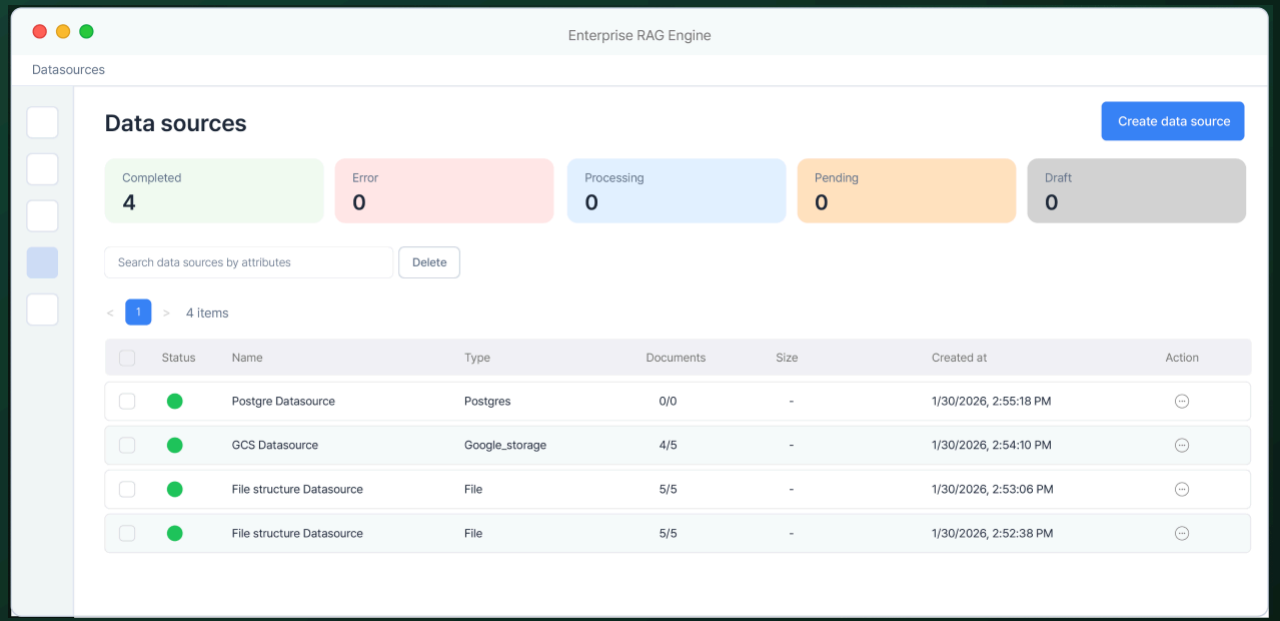
에이전트의 역할, 응답 기준, 업무 처리 방식을 시스템 프롬프트로 설정해 조직별 업무 기준에 맞게 운영합니다.

에이전트 활성화 관리

구성한 에이전트를 활성화하거나 비활성화하여 운영 적용 여부를 간편하게 제어합니다.

Enterprise RAG Engine : 내부 데이터를 신뢰 가능한 에이전트 응답 근거로 전환

Enterprise RAG Engine은 기업 내부에 흩어진 문서와 데이터 소스를 에이전트가 활용할 수 있는 검색 기반 지식 체계로 전환합니다. 다양한 데이터 소스를 연결하고, 문서를 처리·청킹·임베딩한 뒤 하이브리드 검색을 통해 업무 맥락에 맞는 응답 근거를 제공합니다.



다양한 데이터 소스 연결

파일, 클라우드 스토리지, PostgreSQL 등 기업 내부 데이터 소스를 연결해 에이전트가 활용할 수 있는 지식 기반을 구성합니다.

문서 처리 및 청킹

문서를 업무 맥락에 맞는 단위로 분할하고 처리하여 검색 정확도와 응답 품질을 높입니다.

하이브리드 검색

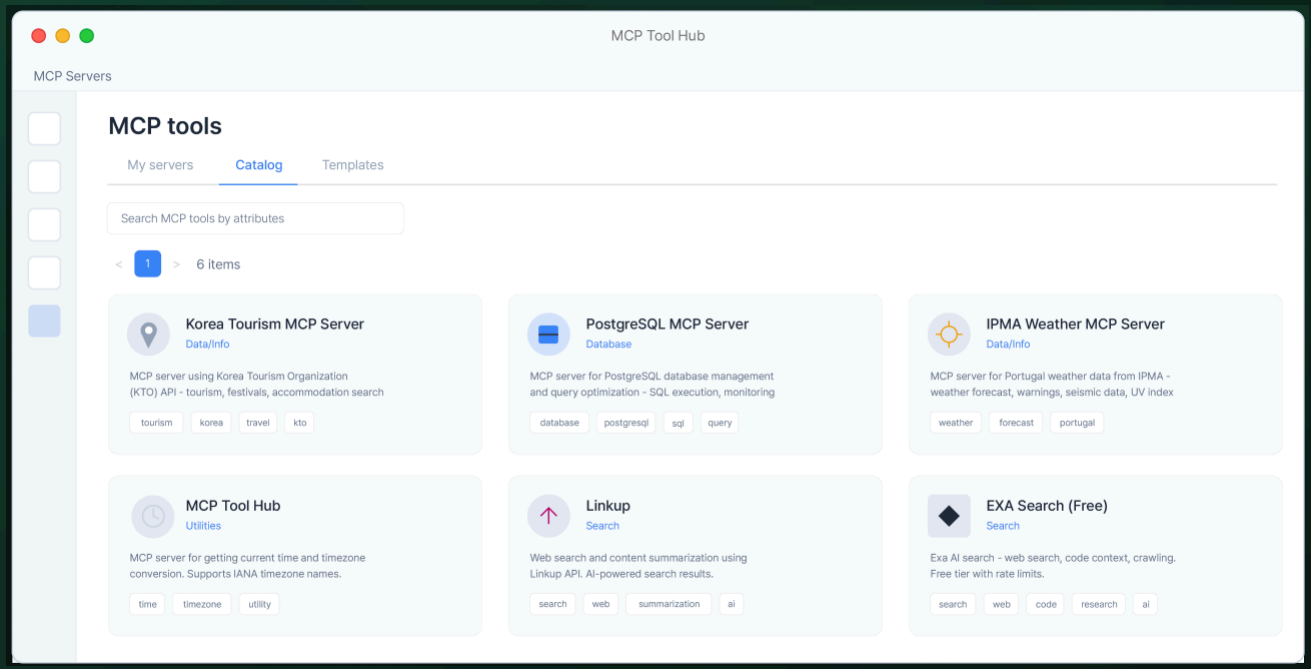
키워드 검색과 벡터 검색을 결합해 도메인 용어, 약어, 문맥을 더 정확하게 반영합니다.

비동기 처리 파이프라인

대규모 문서와 데이터셋을 안정적으로 처리할 수 있는 확장형 파이프라인을 제공합니다.

MCP Tool Hub : 사내 시스템과 에이전트를 안전하게 연결하는 실행 도구 허브

MCP Tool Hub는 에이전트가 단순히 답변하는 것을 넘어 실제 업무 시스템과 상호작용할 수 있도록 지원합니다. 사전에 구성한 MCP 서버와 도구를 관리하고, Agent Builder에서 손쉽게 연결해 조회, 호출, 실행 작업을 수행할 수 있습니다.



MCP 서버 관리

HTTP, STDIO 기반 MCP 서버를 등록하고 관리하여 에이전트가 사용할 수 있는 실행 도구를 구성합니다.

내부 시스템 연계

ERP, CRM, ITSM 등 사내 업무 시스템을 에이전트와 연결해 데이터 조회와 업무 실행을 지원합니다.

카탈로그 기반 생성

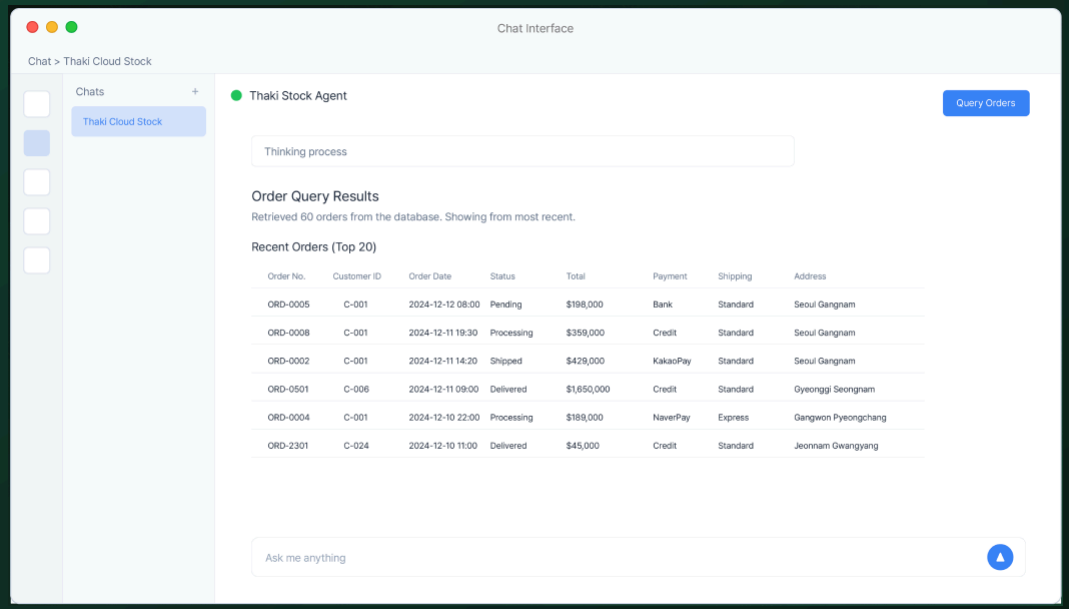
자주 사용하는 도구 연동 구성을 템플릿화해 카탈로그에 등록하고, MCP 서버를 빠르게 생성해 재사용합니다.

인증 및 실행 로그

OAuth 인증과 도구 호출 로그를 기반으로 에이전트의 시스템 접근과 실행 이력을 추적합니다.

Chat Interface : 에이전트와 업무를 수행하는 대화형 실행 인터페이스

Chat Interface는 생성된 에이전트를 실제 업무에 활용하는 대화형 실행 환경입니다. 사용자는 자연어로 질문하거나 업무를 요청하고, 에이전트는 연결된 데이터 소스와 MCP Tool을 기반으로 응답과 실행 결과를 제공합니다.



실시간 에이전트 대화

에이전트와 실시간으로 대화하며 질의응답, 문서 검색, 업무 요청을 수행합니다.

세션 및 대화 이력 관리

이전 대화 맥락과 실행 기록을 유지해 연속적인 업무 흐름을 지원합니다.

응답 근거 확인

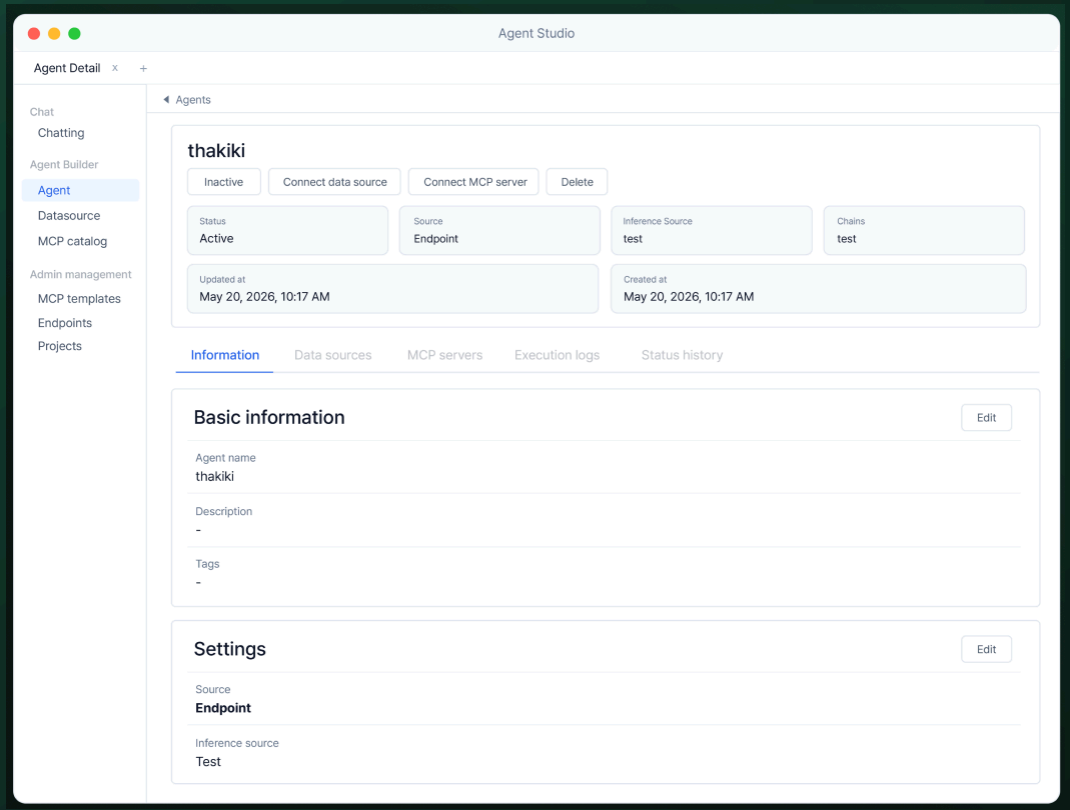
RAG 기반 답변의 출처 문서와 참조 근거를 함께 제공해 응답 신뢰도를 높입니다.

실행 결과 표시

표, 코드, 요약, 결과 메시지 등 업무 요청에 따른 에이전트 실행 결과를 확인할 수 있습니다.

Endpoint Account : 승인된 모델 Endpoint를 에이전트 실행 환경에 연결

Endpoint Account는 에이전트가 사용할 모델 Endpoint를 등록하고 관리하는 연결 계정입니다. 기업은 승인된 Endpoint 정보를 기반으로 에이전트 실행 환경을 구성하고, 내부 정책에 맞는 모델을 선택해 활용할 수 있습니다.



Endpoint 정보 등록

Metis 등에서 생성한 모델 Endpoint URL과 연결 정보를 등록합니다.

모델 실행 환경 연결

등록된 Endpoint를 에이전트에 연결해 기업 내부에서 승인된 모델을 활용할 수 있도록 지원합니다.

Endpoint 계정 관리

프로젝트 또는 운영 환경별로 사용할 Endpoint 계정을 관리해 에이전트 실행 구성을 표준화합니다.

Agent Builder 연계

Agent Builder에서 Endpoint Account를 선택해 특정 에이전트가 사용할 모델 실행 환경을 손쉽게 연결합니다.

THAKI Cloud

5.
Enterprise Agent 운영 과제 및 Use Cases

기업의 주요 업무 영역에서 AI 에이전트를 활용한 구체적인 적용 시나리오를 제공합니다.

기업의 에이전트 도입은 단순한 챗봇 구축이 아니라, 내부 데이터와 업무 시스템을 연결해 실제 프로세스를 자동화하는 운영 과제입니다. 노코드 Agent Builder, Enterprise RAG Engine, MCP Tool Hub, Endpoint Account를 기반으로 보안 요구가 높은 환경에서도 실행 가능한 에이전트 업무 시나리오를 지원합니다.

01 금융·공공·엔터프라이즈 Use Cases

금융권은 여신 데이터와 재무 문서를 분석해 심사 보고서 초안을 생성하고, 공공기관은 법령·정책 데이터를 기반으로 민원 답변 초안을 작성할 수 있습니다. 일반 기업은 사내 규정, 계약 리스크, 코드 리뷰 등 부서별 에이전트를 통해 반복 업무를 자동화할 수 있습니다.

02 사내 시스템 실행 자동화

ERP, CRM, ITSM 등 내부 시스템을 MCP Tool로 연결해 에이전트가 조회, 요청, 등록, 검토와 같은 업무 실행을 지원할 수 있습니다.

03 현업 맞춤형 업무 에이전트 구성

사용자는 생성된 MCP Tool과 데이터 소스를 에이전트에 연결하고, 업무 목적에 맞는 지침을 설정해 부서별 업무 에이전트를 빠르게 구성할 수 있습니다.

04 내부 문서 기반 업무 지원

사내 규정, 계약서, 정책 문서, 기술 문서를 RAG 기반으로 검색하고 요약해 업무 담당자가 신뢰할 수 있는 응답 근거를 확보할 수 있습니다.

THAKI Cloud

Appendix: High-Level Architecture

Appendix: High-Level Architecture

01 프론트엔드

React · TypeScript · Vite/Rspack · TailwindCSS 기반 AI 에이전트 셀프서비스 포털. AI 에이전트 빌더 · 대화형 채팅(WebSocket) · 데이터소스 관리 · MCP 서버 관리 · 프로젝트/IAM

02 에이전트 레이어

FastAPI · Python · LangGraph · Pydantic v2 · Go(Audit Service). Agent Orchestration · RAG Pipeline · Chat Streaming · MCP 서버 라이프사이클 · Auth/ABAC · 멀티테넌시

03 오케스트레이션 & 파이프라인

Apache Airflow(KubernetesExecutor) · Kubernetes · Helm · Argo CD. 문서처리 파이프라인(파싱→청킹→임베딩→벡터저장) · MCP 서버 K8s 배포 · 멀티클러스터 관리 · GCS/RDB 동기화

04 워크로드 관리

PostgreSQL · Qdrant(벡터DB) · NFS · vLLM · Jina Embeddings. 관계형 데이터 · 벡터 임베딩 & 하이브리드 검색(BM25+Dense) · 파일 스토리지 · LLM inference · 임베딩 생성