

인공지능 컨설팅 지원 플랫폼

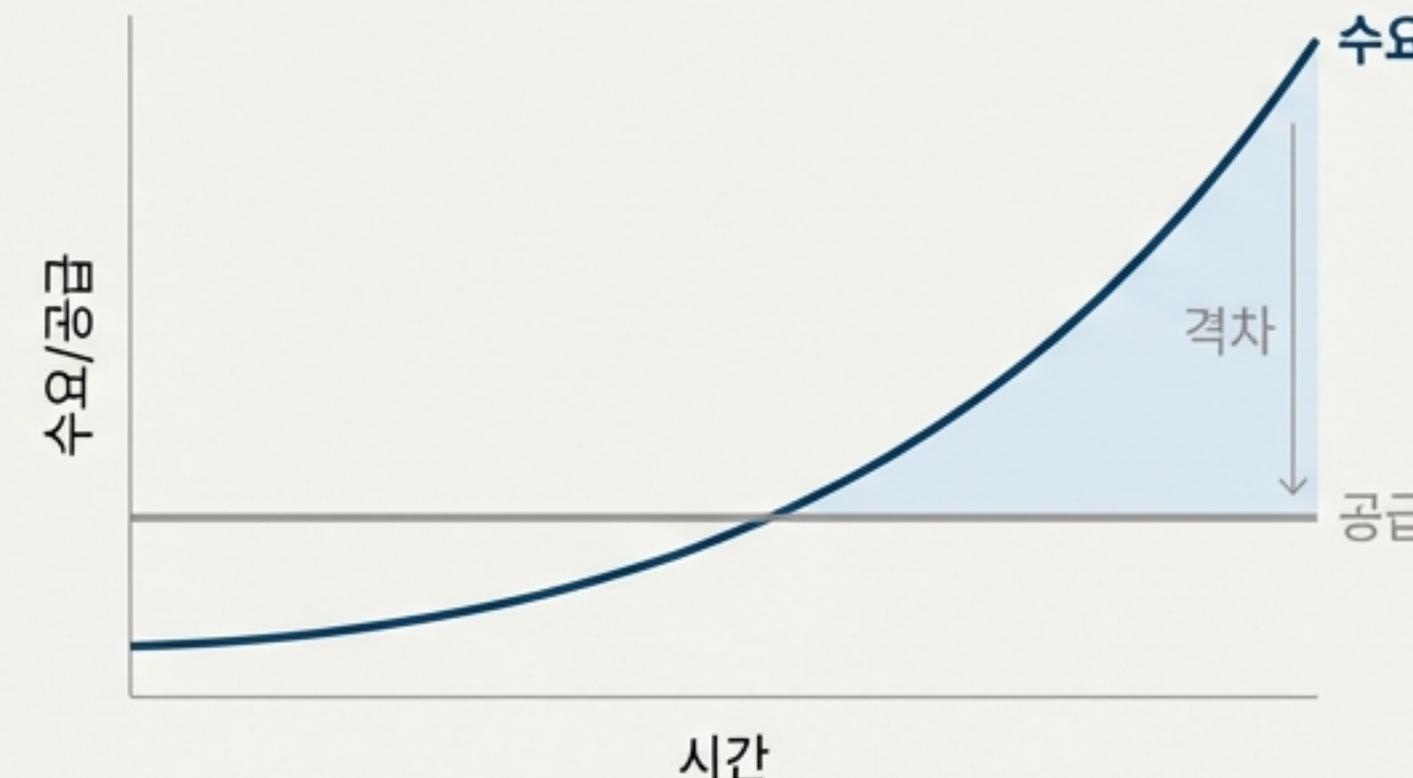
기술 아키텍처 및 워크플로우 분석

문서 버전: 1.2 | 작성일: 2025년 12월 2일

급증하는 AI 컨설팅 수요, 부족한 전문가: 플랫폼의 역할

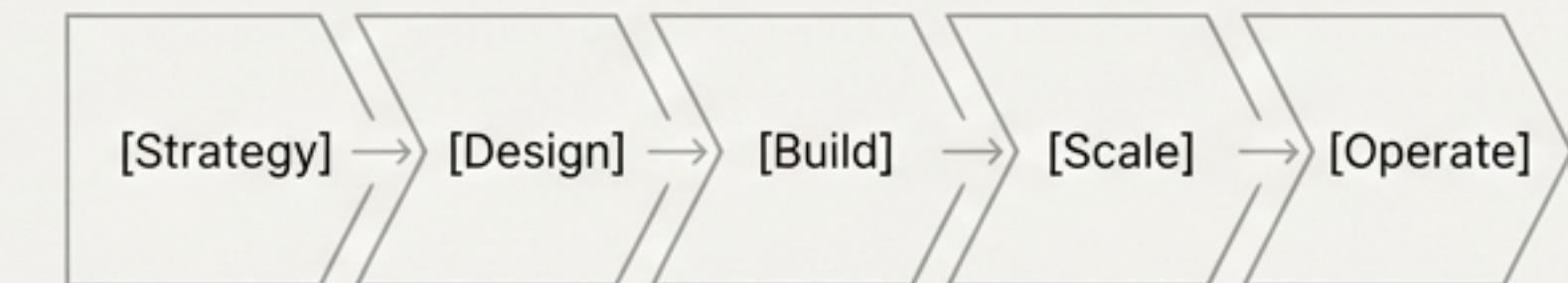
시장의 기회와 제약

AI 전환(AX) 컨설팅 서비스 수요는 폭발적으로 증가하고 있으나, AI 인프라 구축과 전략 수립을 이끌 전문 컨설턴트의 공급은 매우 부족한 상황입니다.



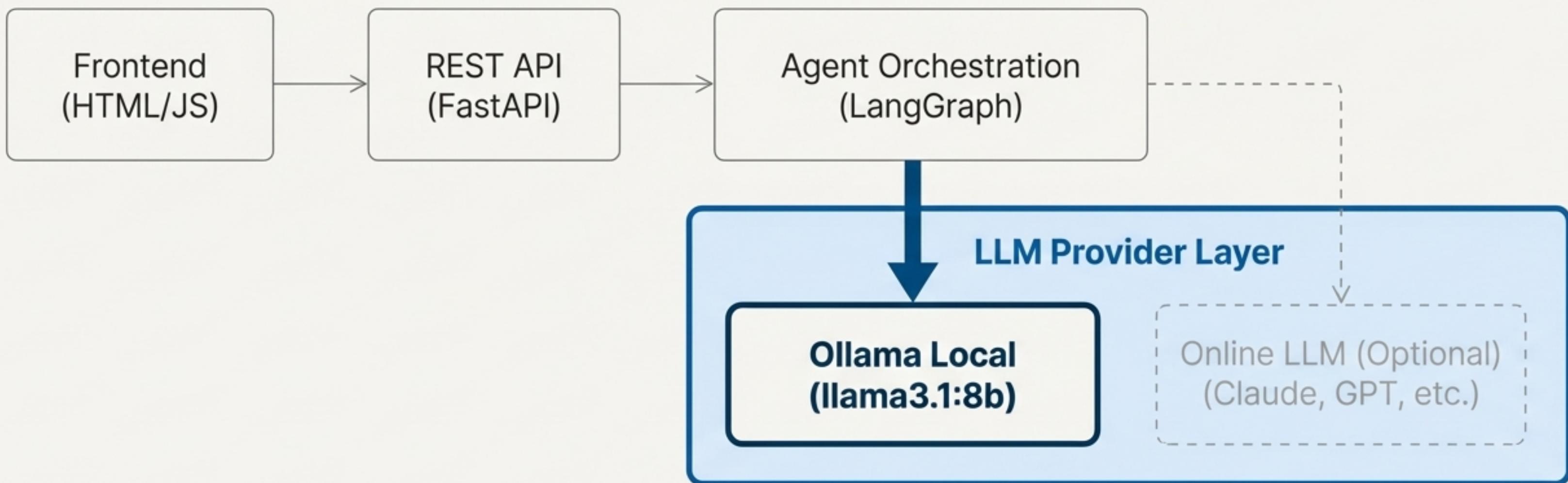
자동화된 5단계 컨설팅 프레임워크

본 플랫폼은 인간 컨설턴트와 멀티 AI 에이전트가 협업하여, 체계적인 5단계 접근법에 기반한 AI 컨설팅 업무를 자동화하고 정교한 결과물을 도출하도록 설계되었습니다.



아키텍처의 핵심: 보안 중심의 하이브리드 LLM

민감한 기업 데이터의 외부 유출을 원천적으로 차단하기 위해,
보안을 최우선으로 고려한 하이브리드 LLM 아키텍처를 채택했습니다.



Ollama 기반 로컬 LLM: 완벽한 데이터 통제와 신뢰성 확보

핵심 구성 요소

구성 요소	설정 값	설명
Base URL	http://localhost:11434	Ollama 서버 엔드포인트
Model	llama3.1:8b	기본 추론 모델
Embedding Model	nomic-embed-text	벡터 임베딩 모델
Temperature	0.7	창의성/일관성 균형

보안 및 운영 이점 비교

보안 요소	Local LLM	Online LLM
데이터 유출 위험	없음	존재
네트워크 의존성	없음	있음
응답 지연	낮음	네트워크 상황 의존
비용	초기 설치비용	사용량 기반
모델 커스터마이징	가능	제한적

AI 컨설팅 드림팀: 역할 기반 전문 에이전트

플랫폼은 CrewAI 패턴을 기반으로 5개의 고도로 전문화된 AI 에이전트를 구성하여, 컨설팅 프로세스의 각 단계를 전담하도록 합니다.



최적의 프레임워크 조합: 에이전트 시스템의 기술 기반

LangChain:

LLM 연동 및 체인 구성의 기반 레이어.
프롬프트, 메시지 히스토리 관리.

LangGraph:

에이전트 워크플로우의 상태를 관리하고
전체 프로세스를 오케스트레이션.

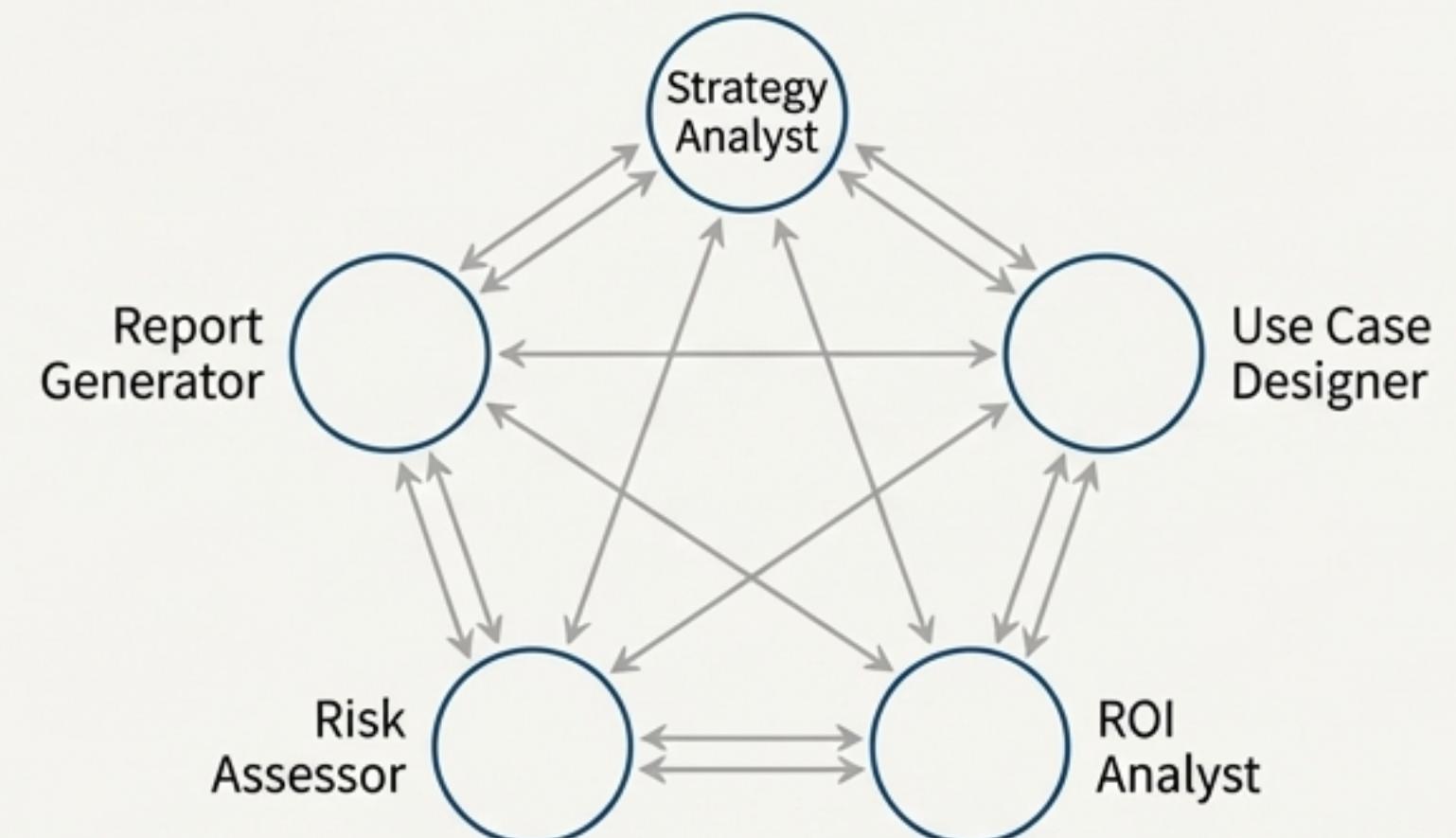
CrewAI:

역할 기반 에이전트 협업 및 태스크 분배 모델
제공.

AutoGen:

인간-AI 협업 메커니즘 및 자율적 피드백
루프에 패턴 적용.

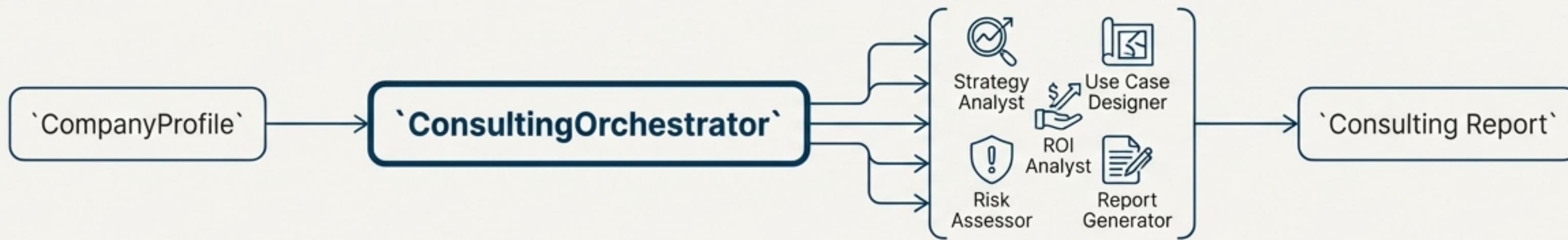
에이전트 간 연결 구조



```
# src/agents/agent_orchestrator.py
def _connect_agents(self):
    for agent in self.agents.values():
        for other_agent in self.agents.values():
            if agent != other_agent:
                agent.connect_agent(other_agent)
```

중앙 제어 시스템: `ConsultingOrchestrator`

전체 컨설팅 워크플로우를 관리하고, 멀티 에이전트 협업을 조율하며,
인간 전문가와의 상호작용을 지원하는 중앙 제어 컴포넌트입니다.



```
# src/agents/agent_orchestrator.py
class ConsultingOrchestrator:
    """
    멀티 에이전트 협업을 조율하고,
    컨설팅 워크플로우를 관리합니다.
    """

    def __init__(self):
        self.llm_provider = get_llm_provider()
        self.agents: Dict[str, BaseConsultingAgent] = {
            "strategy": StrategyAnalystAgent(self.llm_provider),
            "designer": UseCaseDesignerAgent(self.llm_provider),
            "roi": ROIAnalystAgent(self.llm_provider),
            "risk": RiskAssessorAgent(self.llm_provider),
            "report": ReportGeneratorAgent(self.llm_provider)
        }
```

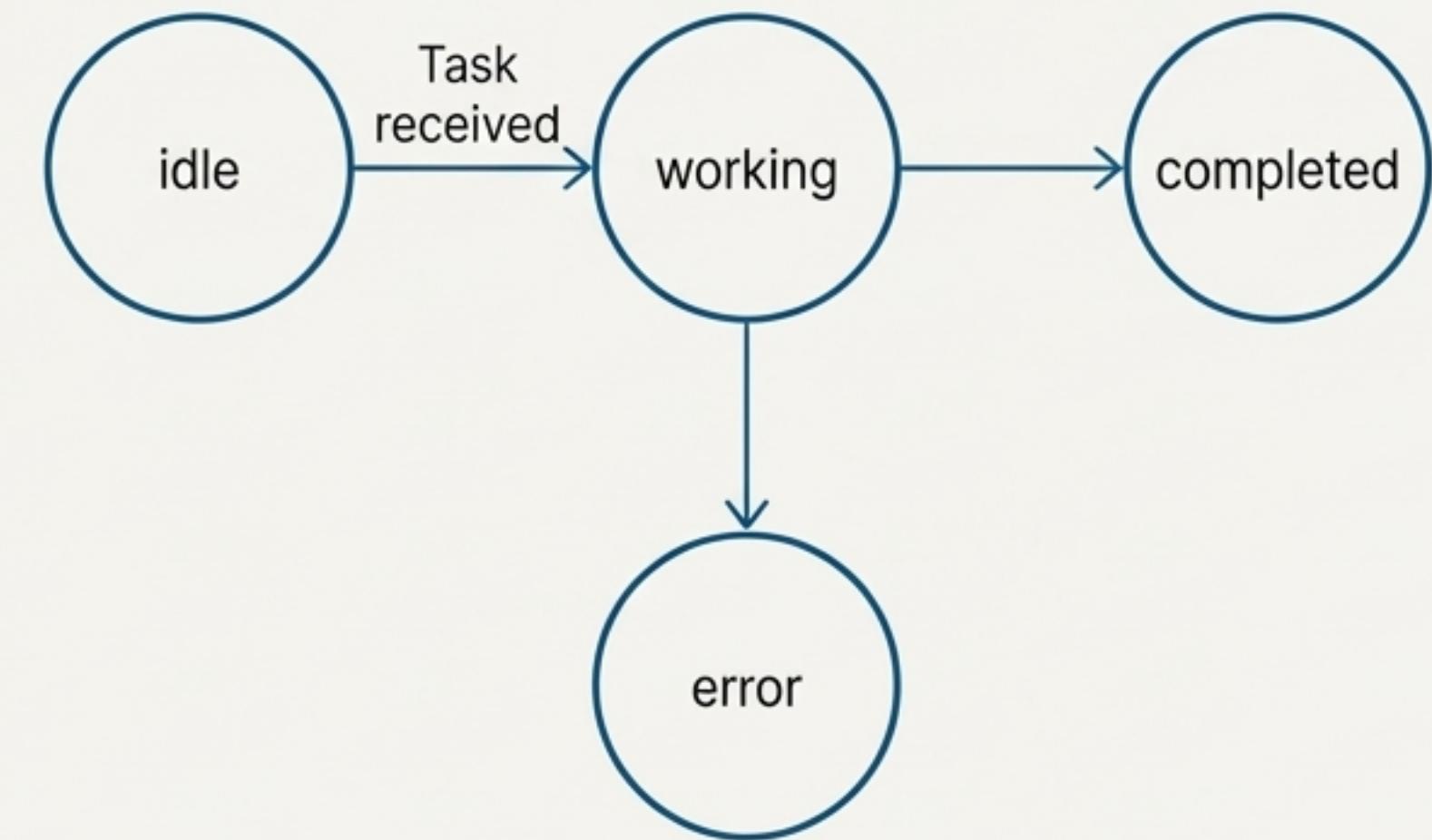
정교한 협업을 위한 프로토콜: 메시징 및 상태 관리

`AgentMessage` 유형

모든 에이전트는 표준화된 메시지 프로토콜을 통해 소통합니다.

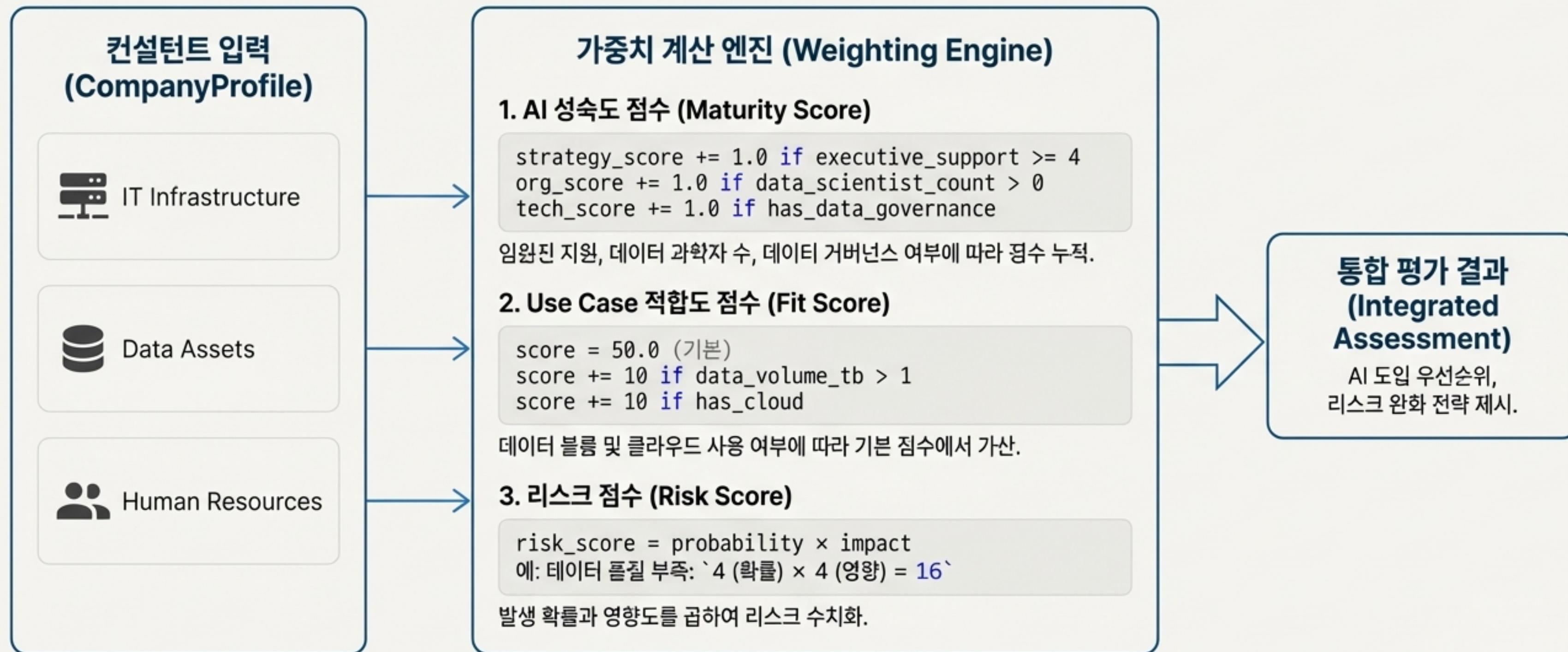
유형	설명	처리 방식
text	일반 텍스트 메시지	LLM 응답 생성
task	태스크 요청	execute() 메서드 호출
result	태스크 결과	결과 저장 및 전달
feedback	피드백 메시지	컨텍스트에 저장
approval_request	승인 요청	인간 검토 대기

에이전트 상태 전이



데이터 기반 의사결정: 가중치 시스템의 작동 원리

명확한 규칙과 데이터에 기반하여 조직의 AI 준비 상태, 유스케이스 적합성, 리스크를 평가하는 시스템입니다.



정량적 분석 기반 시나리오 평가

ROI 분석과 리스크 평가 결과를 종합하여, 각 시나리오의 최종 점수를 객관적인 가중치 공식에 따라 계산합니다.

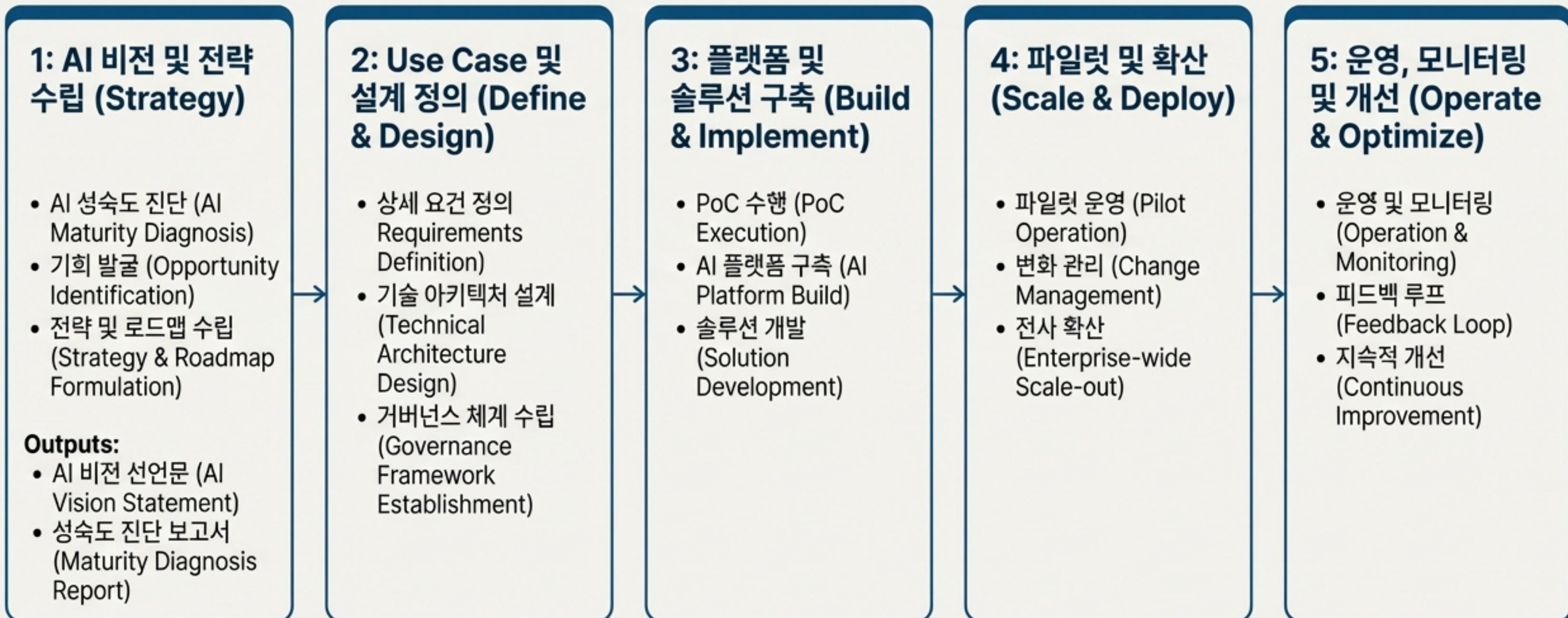
시나리오	예산 비율	리스크 선호도	기간
보수적	0.6x	Low	18개월
균형	1.0x	Medium	24개월
적극적	1.5x	High	36개월

시나리오 종합 점수 계산 로직

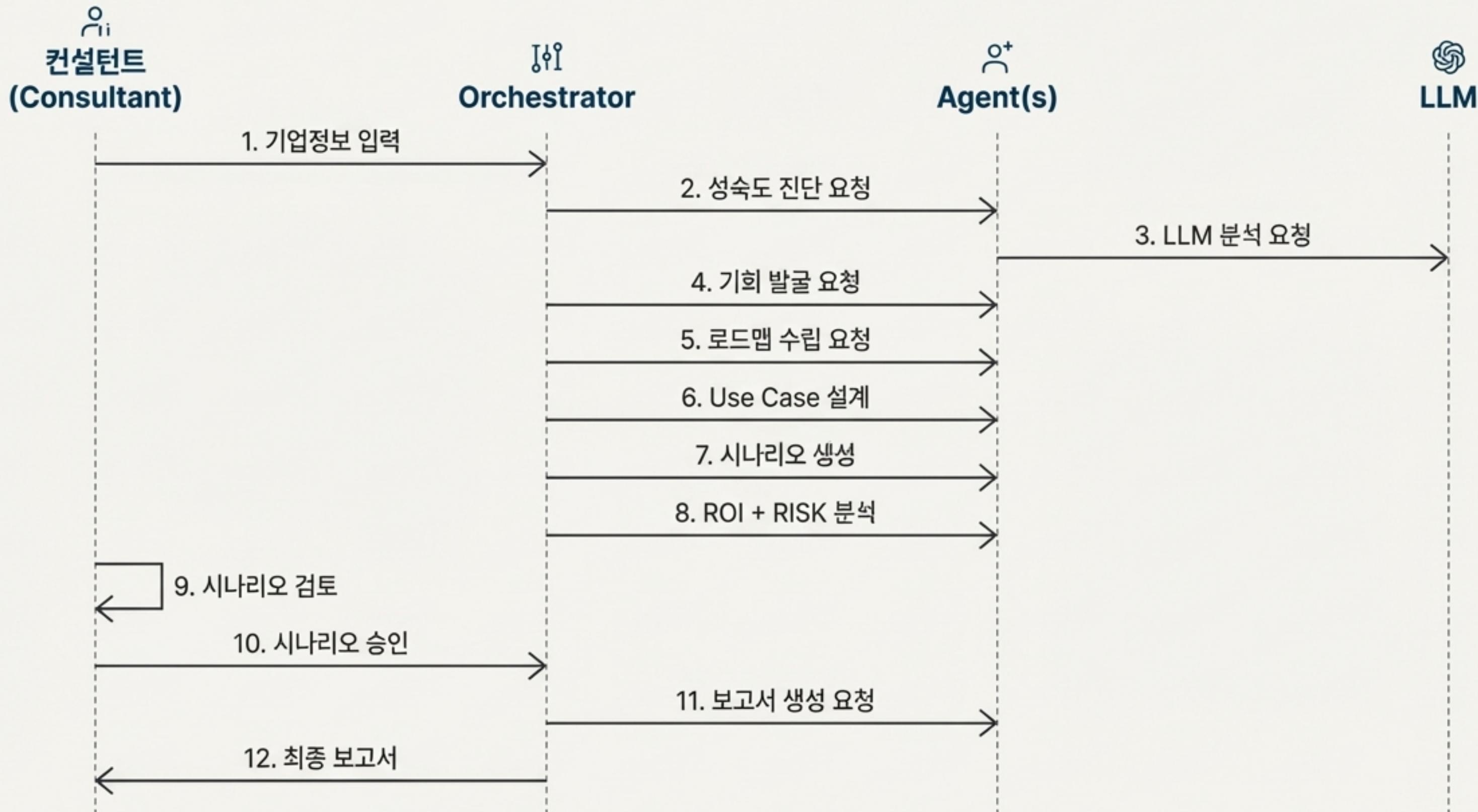
$$\text{종합 점수} = (\text{ROI 점수} \times 0.6) + (\text{리스크 점수} \times 0.4)$$

- **ROI 점수:** $\min(\text{ROI Percent} / 10, 10)$ (ROI 60% 가중치)
- **리스크 점수:** $10 - \text{Total Risk Score}$ (리스크 40% 가중치, 낮을수록 높음)

검증된 방법론: 5단계 컨설팅 프레임워크



End-to-End 워크플로우 실행 흐름



최종 산출물: 데이터 기반의 종합 컨설팅 리포트

Executive Summary 구조

경영진의 빠른 의사결정을 위한 핵심 요약본

- 프로젝트 개요
- AI 성숙도 진단 결과
- 시나리오 분석
- 권고사항 및 Next Steps

전체 보고서 구조

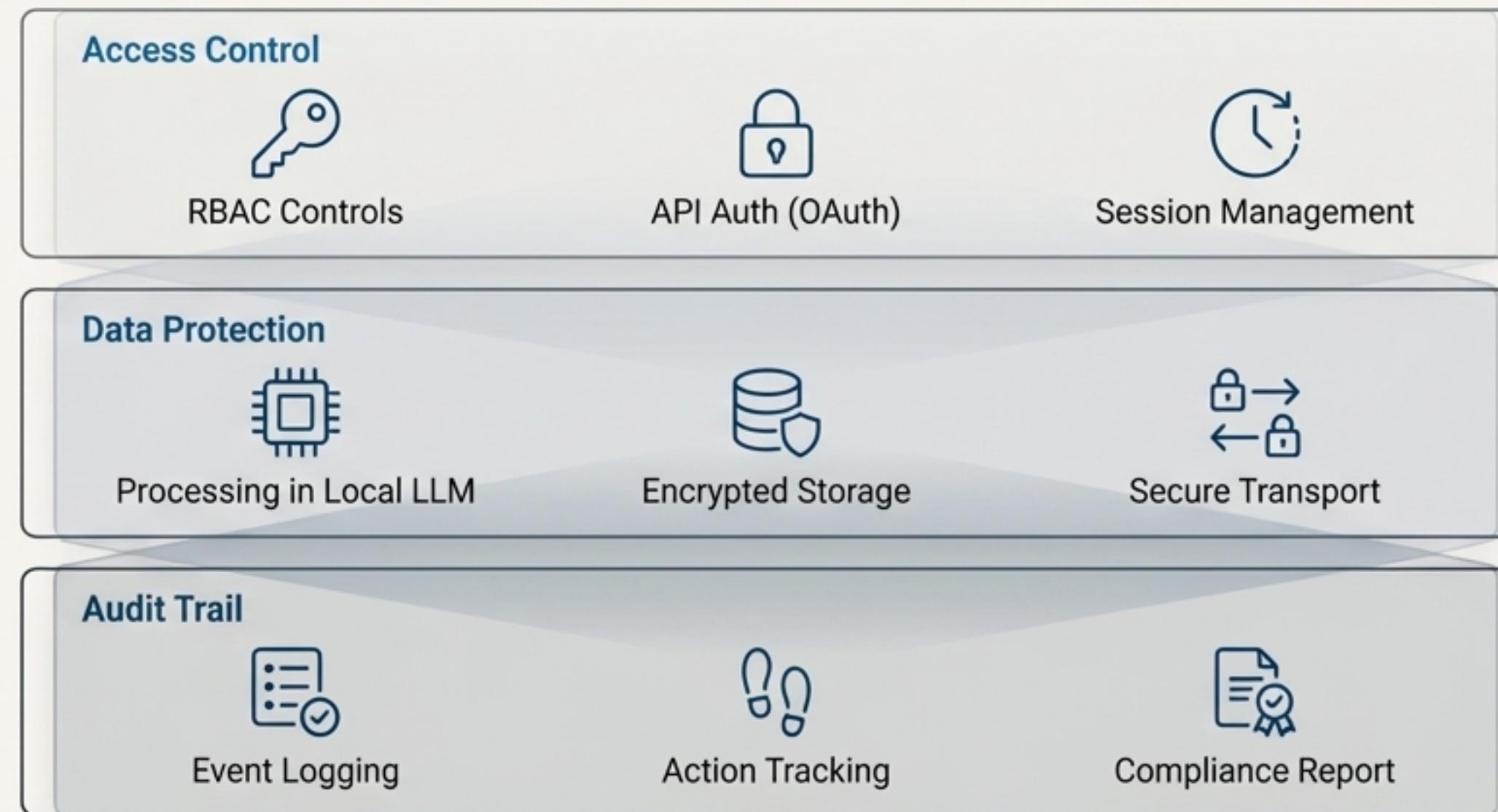
상세 분석 데이터와 실행 계획을 포함한 종합 보고서

- 개요: 배경, 목적, 범위
- 현황 분석: 성숙도, 인프라, 조직, 데이터 자산
- AI 전략 수립: 비전, 핵심 Use Case, 우선순위
- 실행 계획: 시나리오 분석, 로드맵, 투자 계획
- 기대 효과: 정량/정성 효과, ROI 분석
- 리스크 관리: 리스크 식별, 완화 전략

엔터프라이즈급 보안 및 거버넌스 통합

모든 프로세스는 MLOps 표준을 준수하며, 강력한 데이터 보호 및 감사 추적 기능을 통해 신뢰성을 보장합니다.

Data Protection Architecture

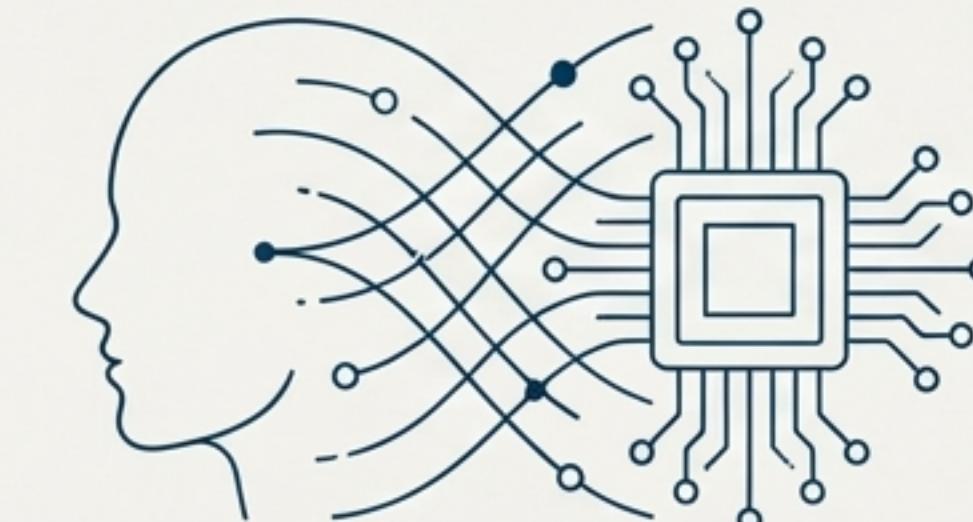


모든 작업 단계는 AuditEventType에 따라 기록되며, RBAC(최소 권한 원칙) 및 파이프라인 보안 스캐닝(Snyk, Trivy) 표준을 준수합니다.

인간의 전문성과 AI의 분석력을 결합한 차세대 컨설팅

핵심 특징

- 보안 중심 설계:** Ollama 기반 Local LLM으로 기업 데이터 완벽 보호 
- 역할 기반 협업:** 5개 전문 에이전트의 정교한 분업과 협력 
- 가중치 기반 분석:** 입력 데이터의 정량적 평가를 통한 객관적 인사이트 
- 자동화된 워크플로우:** 검증된 5단계 컨설팅 프레임워크 자동 실행 
- 종합 리포트 생성:** 모든 분석 결과를 통합한 전문 보고서 자동 생성 



플랫폼 미션

인간 컨설턴트의 전략적 통찰력과 AI의 신속하고 깊이 있는 데이터 분석 능력을 결합하여, 모든 기업이 성공적인 AI 전환을 이룰 수 있도록 지원하는 것을 목표로 합니다.