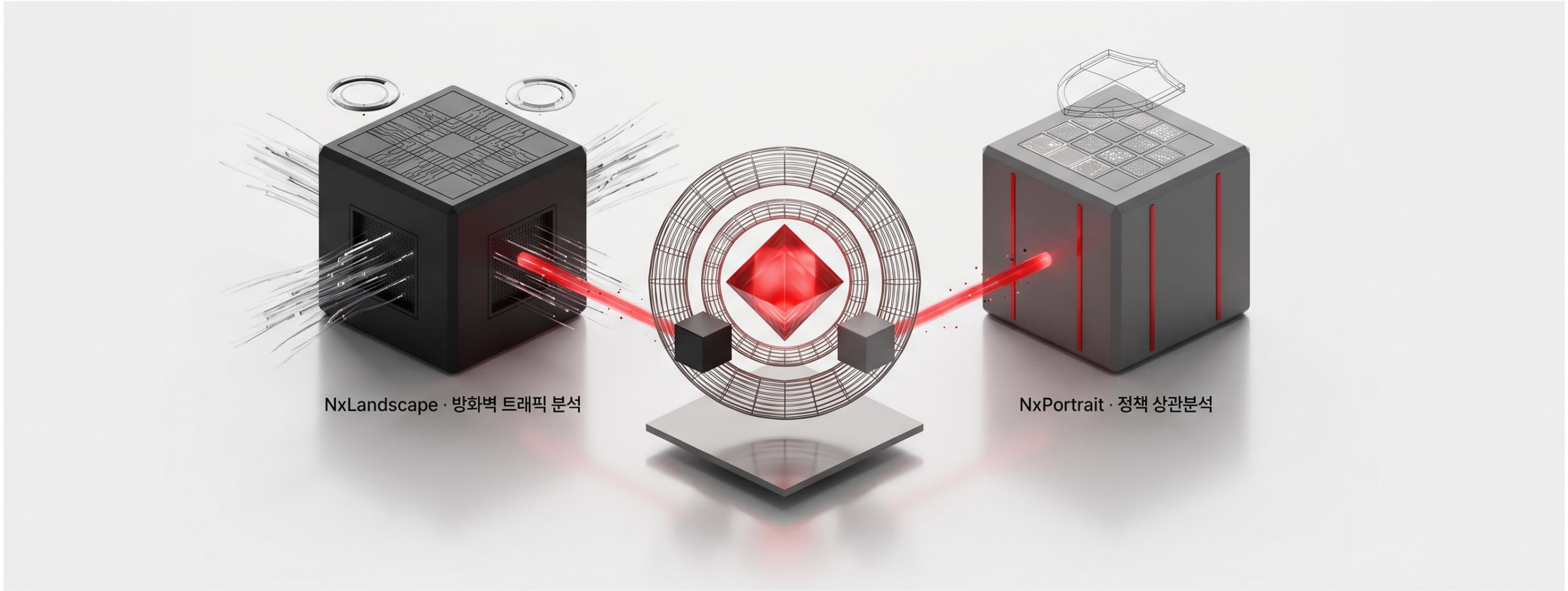



NEXUS.AX

# 분석과 정책을 자율 실행으로 잇는 AI Agent 엔진

NxLandscape · NxPortrait를 자율 실행 체계로 완성합니다

Executive Proposal for Enterprise Customers

# 방화벽 트래픽 분석과 정책 상관분석은 이미 가동 중입니다


NxLandscape · 방화벽 트래픽 분석


NxPortrait · 정책 상관분석

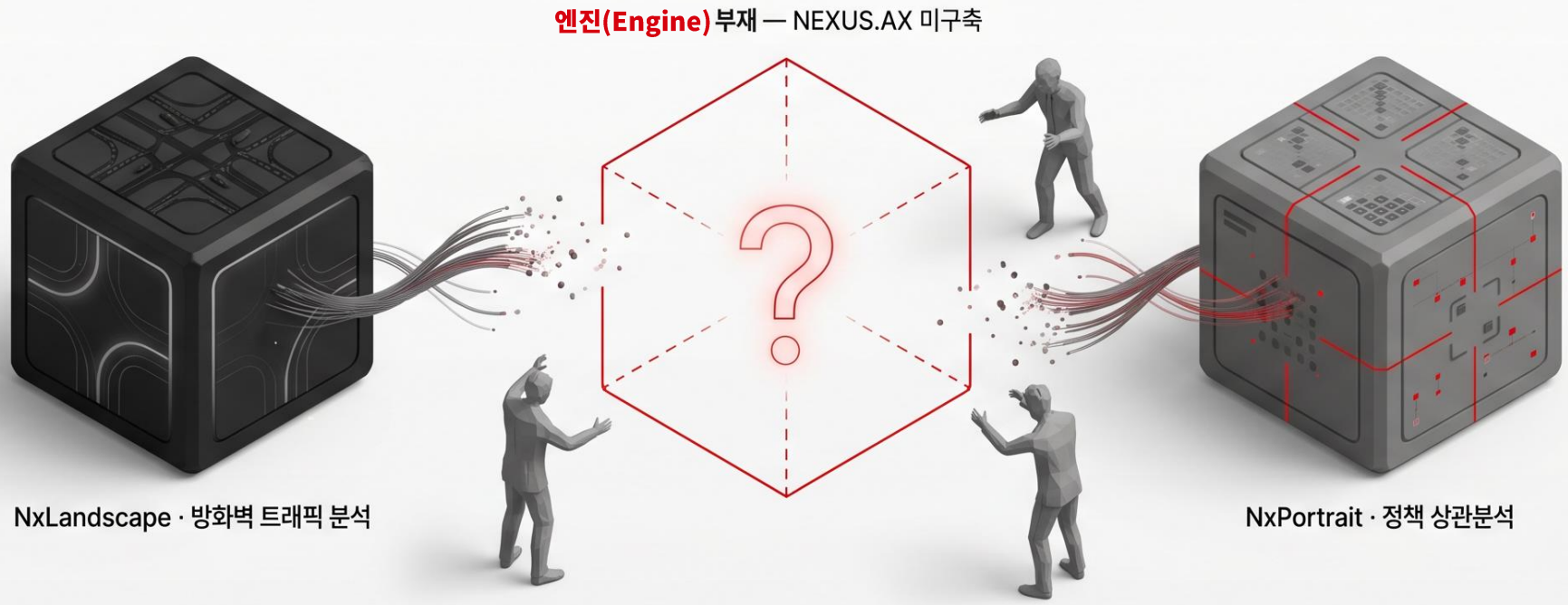
## 실시간 감지 — 이상징후 이벤트

- **C2 통신**
  외부 명령제어 채널 탐지
- **Slow DDoS**
  저속 분산 공격 패턴 식별
- **이상 트래픽**
  임계 초과·비정형 흐름 포착
- **악성 행위 시그널**
  알려진/미지의 위협 시그니처

## 자동 도출 — 4대 취약 정책

- **과다 허용** (Over-permissive)
  광범위 개방으로 공격 통로화
- **미사용** (Unused)
  장기간 트래픽 없는 좀비 룰
- **중복/유사** (Redundant)
  상위 규칙에 가려진 중복
- **기간 만료** (Expired)
  한시 오픈 후 방치된 정책

# 두 자산을 잇는 자율 실행 엔진이 없으면 결국 수동 운영에 그칩니다



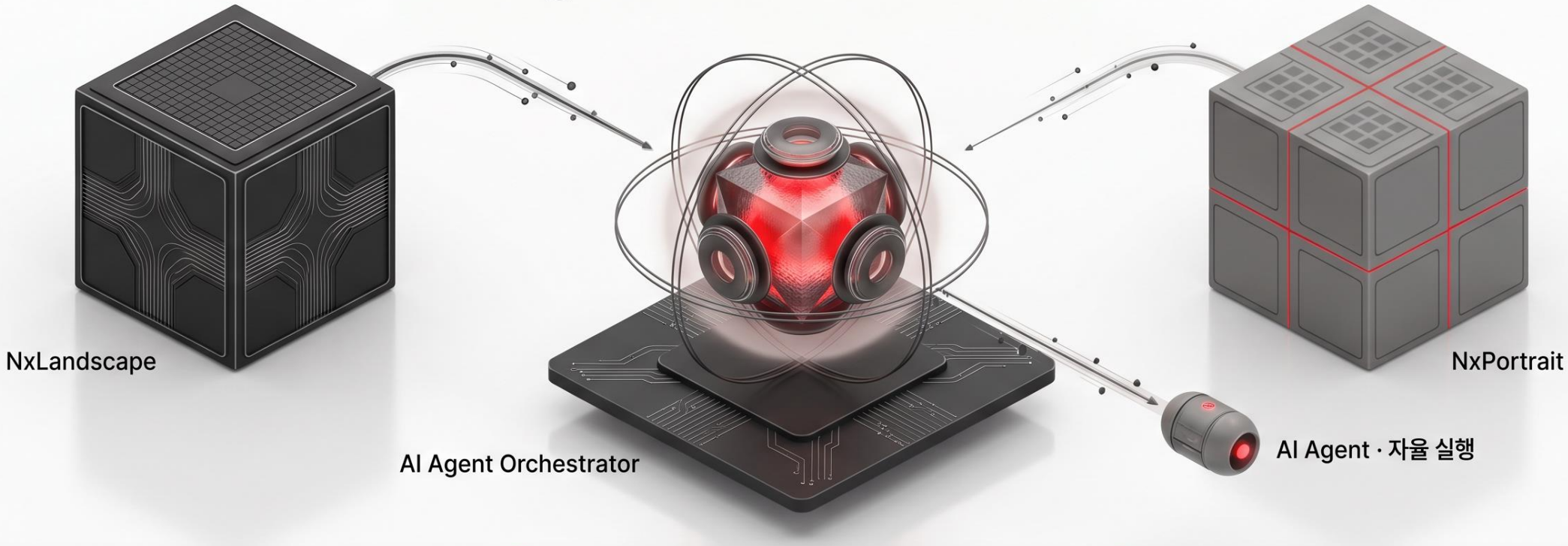

**분석·정책 단절**
— 사람이 매번 두 시스템을 연결해 판단해야 합니다

**Agent 응답 비일관성**
— 상황·정책 미반영 위험이 존재합니다

**운영 부담 누적**
— 인력 의존이 고착화됩니다

NEXUS.AX

# NEXUS.AX는 분석과 정책을 자율 실행으로 잇는 AI Agent Orchestrator입니다




**상황 인지 통합** — 방화벽 트래픽 분석을 Agent 실시간 판단 입력으로 활용합니다

**정책 통제 통합** — 정책 상관분석 결과를 Agent 행동 기준으로 강제합니다

**자율 실행 전환** — 사람의 수동 개입 없이 분석에서 실행까지 하나의 흐름으로 이어집니다

# NEXUS.AX는 3대 모듈로 분석과 정책을 자율 실행으로 변환합니다


**Context Filter**
— 이상징후 관련 정보 자동 선별

**Semantic Harness**
— Agent에 정책을 동적으로 적용

**Adaptive Model Router**
— 쿼리별 모델 자동 라우팅

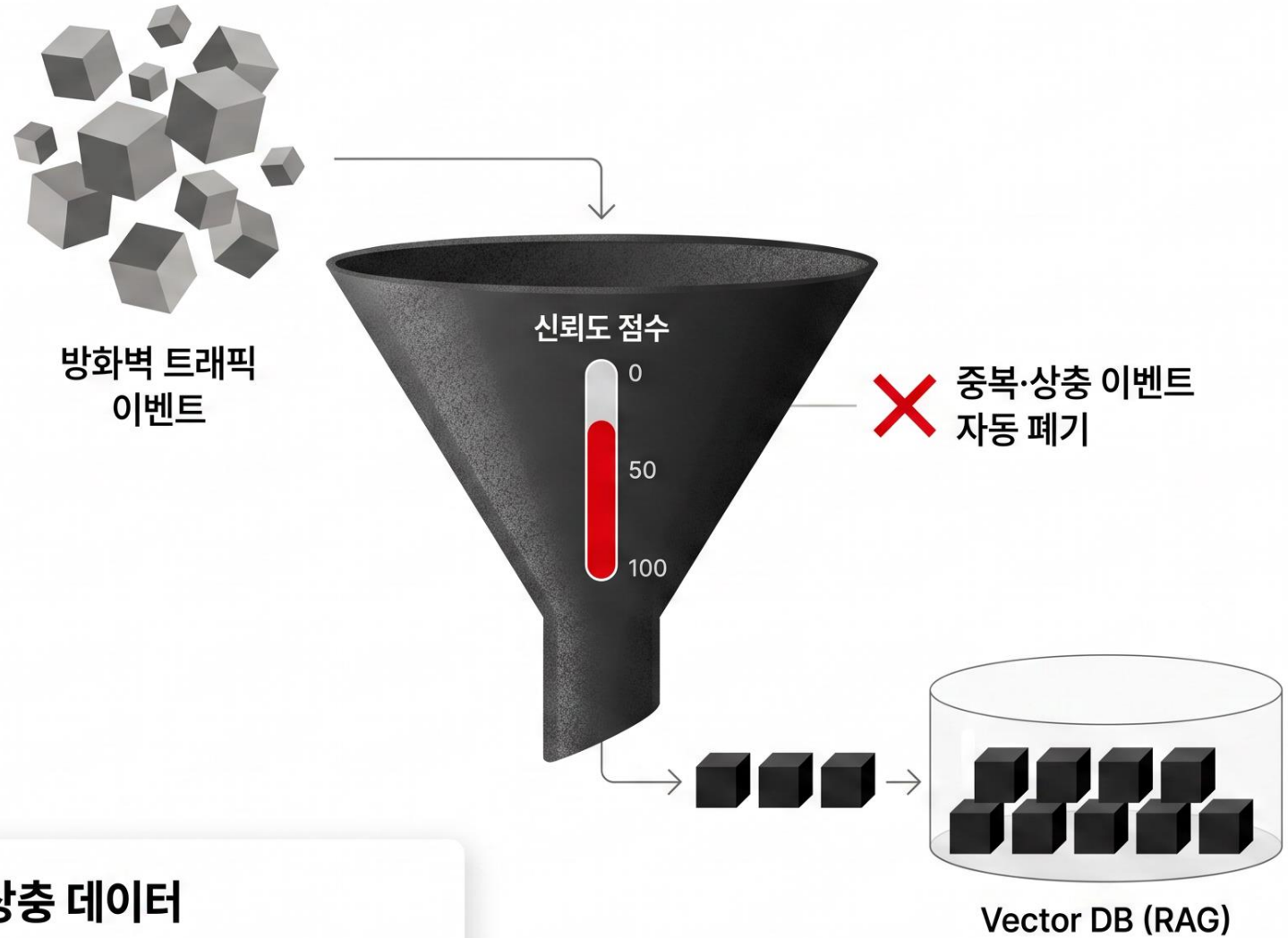
NEXUS.AX

Agentic Curation Pipeline

# AI가 학습할 진짜 정보만 골라냅니다

**Context Filter (벡터 DB 동기화 · RAG)**

NxLandscape의 방화벽 트래픽 이벤트를
신뢰도 점수 기반으로 자동 큐레이션합니다




### 이상징후 발생 시

관련 매뉴얼과 최신 트래픽
데이터를 자동 동기화합니다

### 중복·상충 데이터

신뢰도 점수 기반 자동 폐기로
노이즈를 제거합니다

NEXUS.AX

# 가드레일과 하네스로 AI Agent를 안전하게 통제합니다

Dynamic Policy Enforcement

## Guardrail · 외부 경계 통제

Static Boundary — 일탈 차단

**역할** — 외부 경계 설정

**강점** — 명확한 일탈 차단

## Harness · 내부 정책 인라인 적용


Inline Enforcement — 정책 동적 강제

**역할** — Agent에 정책을 직접 적용

**강점** — 자율성 유지하며 정책 준수

NEXUS.AX는 Guardrail과 Harness를 동시에 적용하여, AI Agent의 자율성을 제한하지 않으면서도 정책 준수를 보장합니다.

NEXUS.AX

PIPELINE 03

# Agent가 스스로 판단하되, 모든 결정은 추적됩니다

## Agentic AI Workload Optimization

Agentic AI

AI Agent는 관찰·추론·행동·성찰의 자율 사이클을 수행하며, Adaptive Model Router가 쿼리 특성에 따라 모델을 자동 선택하고, Agent Trace가 모든 의사결정을 추적합니다.

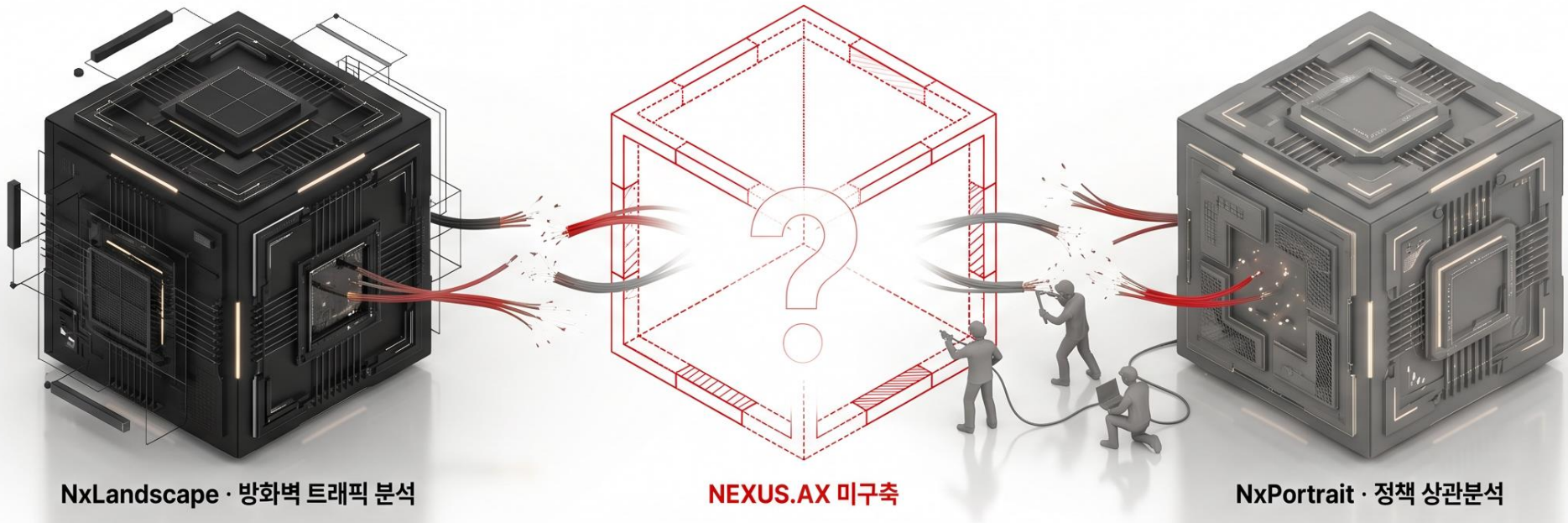
Adaptive Model Router + Agent Trace


**1) Adaptive Routing —**
쿼리 복잡도 기반 비용·보안 균형 자동 결정

**2) Agent Observability —**
거버넌스를 위한 전 의사결정 추적

NEXUS.AX

# NEXUS.AX 구축이 미뤄질수록 확보한 두 자산의 활용도가 정체됩니다



NxLandscape · 방화벽 트래픽 분석

NEXUS.AX 미구축

NxPortrait · 정책 상관분석

### 자산 활용 정체
분석과 정책이 자율 실행으로 연결되지 못해 가치 실현이 지연됩니다

### 수동 운영 고착화
인력 의존이 지속되어 운영 효율 개선이 어렵습니다

### 보안 사각지대 누적
정책 위반 탐지가 사후 대응에 머무릅니다

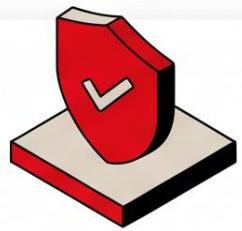
### 자율 실행 격차 확대
시장 대비 보안 운영 자동화 격차가 벌어집니다

NEXUS.AX

# 6개월 3단계로 NEXUS.AX 자율 실행 체계를 완성합니다

Phase 1

**M1~M2**



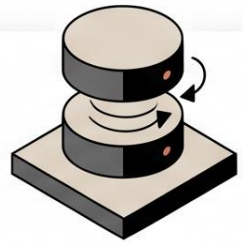
## Dynamic Policy Enforcement

- NxPortrait Semantic Harness 구축
- Guardrail + Harness 동시 적용
- 4대 취약 정책 자동 검증

**보안 가치 확보**

Phase 2

**M3~M4**



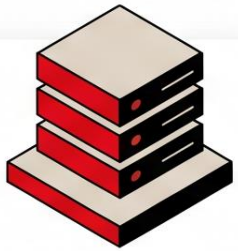
## Agentic Curation

- NxLandscape Context Filter
- Vector DB 실시간 동기화
- 이상징후 정보 자동 선별

**품질 가치 확보**

Phase 3

**M5~M6**



## Workload Optimization

- Adaptive Model Router
- 온프레미스 · 클라우드 자동 라우팅
- Agent Trace 관찰가능성 통합

**비용 효율 확보**

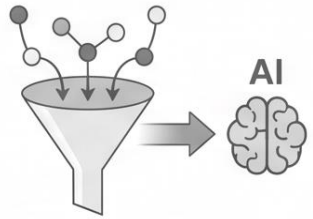
각 단계는 보안, 품질, 비용 가치를 순차적으로 확보하며
자율 실행 체계를 완성합니다

NEXUS.AX

# 3가지 핵심 Q&A로 NEXUS.AX의 본질을 정리합니다

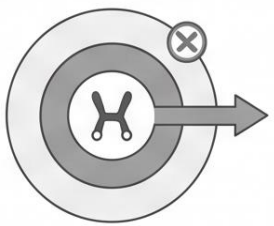
**Q: NxLandscape의 분석 데이터가 AI Agent의 판단력을 어떻게 강화합니까?**

**A:** Context Filter가 이상징후 발생 시 관련 매뉴얼과 최신 트래픽 데이터를 Vector DB에 자동 동기화하여, AI Agent가 실시간 상황을 정확히 이해하고 판단합니다.



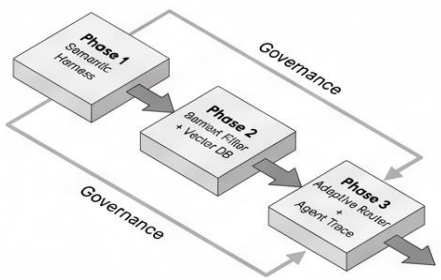

**Q: NxPortrait 정책 강제가 AI Agent의 자율성을 해치지는 않습니까?**

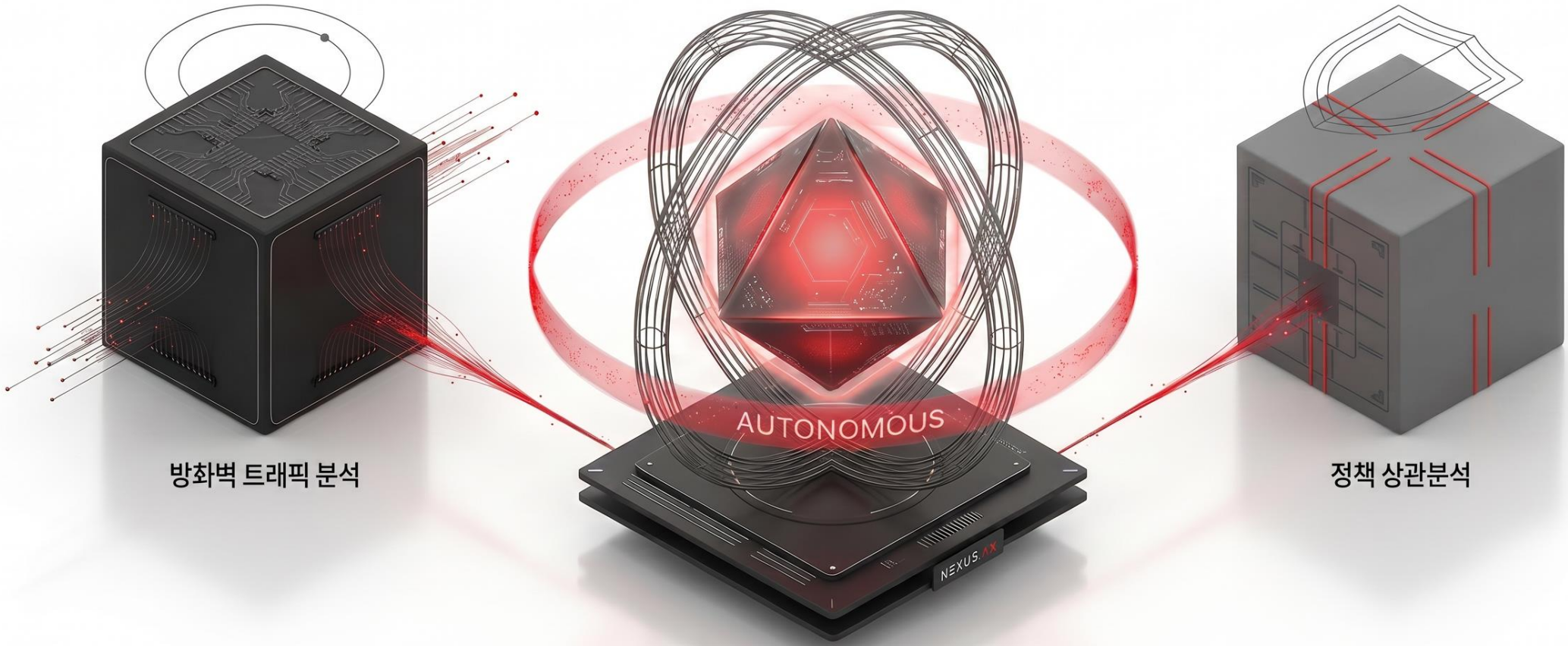
**A:** 가드레일은 외부 경계로 일탈을 차단하고, 하네스는 내부에서 정책을 인라인으로 적용합니다. 두 개념의 조합으로 자율성을 유지하면서도 정책 준수를 보장합니다.



**Q: 각 단계의 산출물과 거버넌스는 어떻게 확보됩니까?**

**A:** Phase 1은 Semantic Harness로 정책을 인라인 강제하고, Phase 2는 Context Filter와 Vector DB로 응답 품질을 확보하며, Phase 3는 Adaptive Router와 Agent Trace로 비용 최적화와 전체 의사결정 추적을 동시에 보장합니다.






방화벽 트래픽 분석

정책 상관분석

**두 자산은 이미 가동 중입니다.**
**NEXUS.AX 엔진을 더하면 자율 실행 체계가 완성됩니다.**



NEXUS.AX

# 다음 과제: 보안 지식의 온톨로지화로 AI Agent의 가설·추론을 구조화합니다

Knowledge Graph for Agentic Reasoning

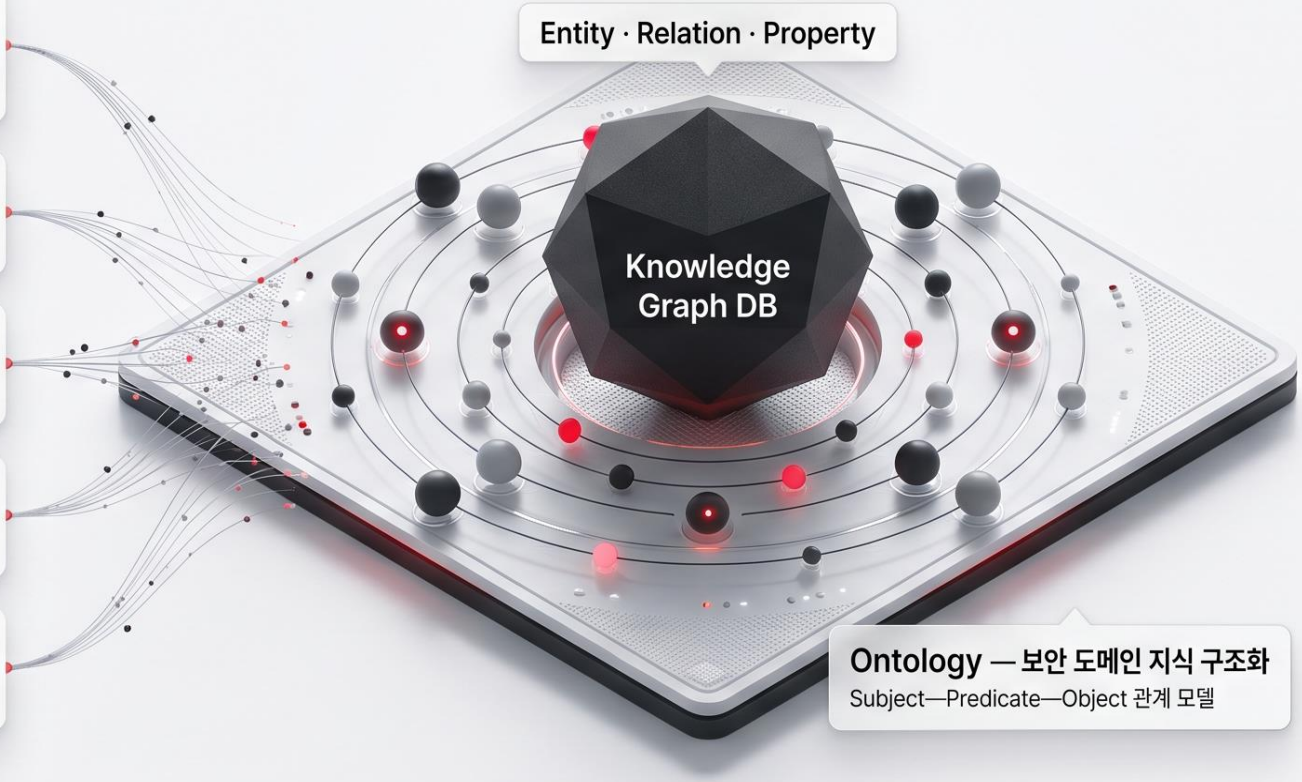
**01 IP 자산 레이블링**
— CMDB·ITAMS 연동, SCO(기밀·민감·오픈) 스코어링

**02 보안장비 토폴로지**
— N-S, E-W 배치 정보

**03 정책 상관분석**
— 보안 장비 내 정책 간 관계 정보

**04 트래픽 세션·이상징후**
— 정책 내 객체 단위 세션 흐름

**05 ASM·TI Observation**
— 외부 공격면 및 위협 인텔리전스




NEXUS.AX inference flow

1) Hypothesis · 가설 생성

2) Evidence Retrieval
· 그래프 근거 검색

3) Reasoning Output
· 추론 결과

**5가지 정보 원천을 그래프DB로 온톨로지화하면, AI Agent의 모든 가설과 추론이 명확한 근거 위에서 수행됩니다.**

NEXUS.AX