



기업 업무를 위한 통제된 AI 실행

기업 업무 지식 자산·실행 권한·실무 도입

업무는 확장하고, 업무 지식은 기업의 자산으로.

기술 백서 | 한국어판

2026년 10월 18일

www.vibepackr.com

목차

01 업무는 확장하고, 업무 지식은 기업의 자산으로.	6
02 책임 있는 실행 경계를 갖춘 기업 AI	9
03 하나의 보호된 코어와 구분된 준비·Work 경로	12
04 설치에서 운영까지: 필요한 도구 선택	15
05 GAPE: 소스 발견·대조·검토	18
06 Integration Helper: 준비·검증·인계	20
07 SDK Engine: 추가 권한 없는 확장	22
08 로컬 SDK 예제: 입력·산출물·재현성	24
09 헤드리스 운영과 사람의 검토 화면	25
10 통제된 실행: 요청에서 검토까지	27
11 신원·접근과 Work Authority	29
12 증거를 통한 검토와 책임 있는 인수	31
13 기업 AI 도입·사용의 규제 감사 검토	33
14 고객·VibePackr·제3자의 책임	34
15 배포·복구: 계산 자원·저장·검증	36

목차

16 Packtory: 상세한 향후 지식 아키텍처	38
17 기업 평가: 확장 전에 의존성 확인	40
18 빙산: 실행 아키텍처의 네 계층	42
19 공유 자원과 충돌하는 요청	44
20 시가 할 수 있는 일과 실행이 허용된 일은 다릅니다.	46
21 기업 아키텍처의 통제된 실행	49
22 배포 및 신뢰 경계	52
23 에이전트 침해만으로 권한이 부여되지는 않습니다.	54
24 하나의 아키텍처. 세 가지 읽는 방법.	57
25 로컬 기록 사례: 하나의 식별자를 따라가기	62
26 필요한 매뉴얼 선택: Part.1~8	63
27 네 가지 실무 가이드와 문제 해결 인계	64
28 이 판에서 사용하는 용어	65
29 출처·읽기 경로·판 안내	66

그림 목차

그림 1 · 기존 기업 시스템 안에서의 VibePackr	10
그림 2 · 기본 운영 모델	13
그림 3 · 선언과 준비	17
그림 4 · GAPE: 거버넌스 기반 아키텍처 프로젝트	19
그림 6 · VibePackr 헤드리스 운영	26
그림 7 · 요청에서 실제 실행까지	28
그림 8 · 신원·접근과 Work Authority의 구분	30
그림 9 · 관찰·증거·검증·인수	32
그림 10 · 역할별 공동 책임	35
그림 11 · 운영과 복구	37
그림 12 · 향후 호스팅·공유 구상	39
그림 13 · 다른 출발점에서 시작하는 평가	41
그림 15 · 계층별 아키텍처 참고도	43

그림 목차

그림 17 · 공통 제품과 고객별 구현 책임	21
그림 18 · AI 위험에서 실행 통제로	45
그림 20 · SDK Engine: 거버넌스를 유지하는 확장	23
그림 23 · 사람의 의도에서 통제된 Work까지	14
그림 24 · AI 기능과 배포별 신뢰 경계	53
그림 25 · 기능과 실행 권한의 구분	48
그림 26 · 기업 AI 아키텍처 안에서의 VibePackr	51
그림 27 · XYZ 아키텍처 공간	61
그림 28 · AI·에이전트 침해와 실행 권한	56
그림 29 · Non-SI 연동과 운영 적용	11
그림 30 · 여러 복잡한 영역에서 하나의 사용자 경험으로	7
그림 31 · VibePackr Pack 시스템	8
그림 32 · 설치와 도구 사용 흐름	16

그림 번호는 웹사이트의 참조 식별자를 유지합니다. 모든 도표에 현재 영문 SVG를 사용했습니다.

01 업무는 확장하고, 업무 지식은 기업의 자산으로.

기업의 AI 도입은 구성원의 업무 역량을 확장하고, 그 과정에서 얻은 노하우를 기업 소유의 재사용 가능한 사용자 커스텀 Pack으로 축적하는 데까지 이어져야 합니다.

ERP·CRM·SCM의 기록에 더해, 업무를 실제로 수행하는 방법·판단 기준·예외 대응까지 지식으로 남깁니다. 이러한 암묵지를 증류·검토하고 라벨링하여 통제된 재사용의 기반으로 만듭니다.

증류·구조화

이 지식 자산화 모델의 내부 인텔리전스 코어인 PINM은 업무 경험을 증류·구조화하고, 개념·방법·근거를 연결하는 버텨업 온톨로지를 구성합니다.

사용자 커스텀 Pack으로 라벨링

검토한 업무 방법·문맥·재사용 조건을 사용자 커스텀 Pack으로 구성합니다. Pack에 명확한 식별자·용도·리비전을 부여해 필요한 업무 지식을 찾고 재사용할 수 있게 합니다.

Packtory에 축적·재사용

명시적 등록과 지원되는 Packtory 수명주기에 따라 커스텀 Pack을 관리합니다. 권한이 있는 다른 구성원은 적합한 Pack을 찾아 새로운 업무에 재사용할 수 있습니다.

담당자가 퇴사해도, 업무 지식은 기업에 남도록.

커스텀 Pack에 남긴 업무 지식은 다음 담당자가 활용할 방법·문맥·근거를 제공합니다. 같은 설명을 반복하거나 복잡한 인수인계·교육에 의존하는 부담을 줄이는 기반이 됩니다.

업무 지식 자산의 보유·관리는 기업의 통제 아래.

이 지식 자산을 구축하기 위해 자산 기반을 AI 프로바이더에 넘길 필요는 없습니다. 외부 AI 호출은 별도의 데이터 흐름이며 구성·정책·프로바이더 약관에 따라 관리합니다.

VibePackr는 검증된 Work에서 재사용할 업무 지식을 증류하고 로컬 Packtory에서 지원 Pack을 관리합니다. Pack을 재사용하기 전에 검토·등록하고, 해당 릴리스의 권한과 지원 인터페이스를 적용하세요.

웹사이트에서 이어서 보기

[/enterprise-knowledge](#)

그림 31 · VibePackr Pack 시스템



VibePackr Pack System

Governed capability composition, operational maintenance and availability support.

Keep the Golden image frozen. Add supported capabilities through governed Packs.



02 책임 있는 실행 경계를 갖춘 기업 AI

VibePackr는 고객 소유 인프라, 통제된 실행, 범위가 정해진 적용을 위한 단일 테넌트 기업용 AI 어플라이언스입니다. 지원 클라우드와 기존 환경에서 공급업체 수행 SI 없이 배포하고 운영할 수 있습니다.

통제하는 대상

VibePackr를 통해 전달되는 지원 Work에 대해 보호된 Packr Engine이 해당 Work Authority·정책·범위를 확인하고, 허용된 실행을 통제하며, 결과를 검증·증거·기술 리시트에 연결합니다. 유용한 AI 제안이나 사용할 수 있는 인증정보만으로 작업이 승인되지는 않습니다.

기존 시스템과 조직의 책임

지원 인터페이스·선언형 Contract·통제된 Pack으로 기존 시스템을 연결합니다. 설정·데이터 권리·배포·운영은 고객이 담당하며, 외부 인프라와 AI 서비스는 각자의 책임을 유지합니다. Google Cloud·AWS·Microsoft Azure의 배포 가능 여부와 호환성은 릴리스별로 다르며, 웹사이트는 AWS와 Azure를 시험 중으로 표시합니다.

하나의 유용한 Work부터 평가

업무·허용 입력·대상·책임자·인수 기준을 정의합니다. 실행 전에 제공 제품 버전과 지원 경로를 확인합니다. 성공 결과 뿐 아니라 거절과 미완료 결과도 보존한 뒤, 관찰된 결과가 업무 요구를 충족하는지 판단합니다.

웹사이트에서 이어서 보기

/

[/architecture/](#)

[/guides/poc/](#)

그림 1 · 기존 기업 시스템 안에서의 VibePackr

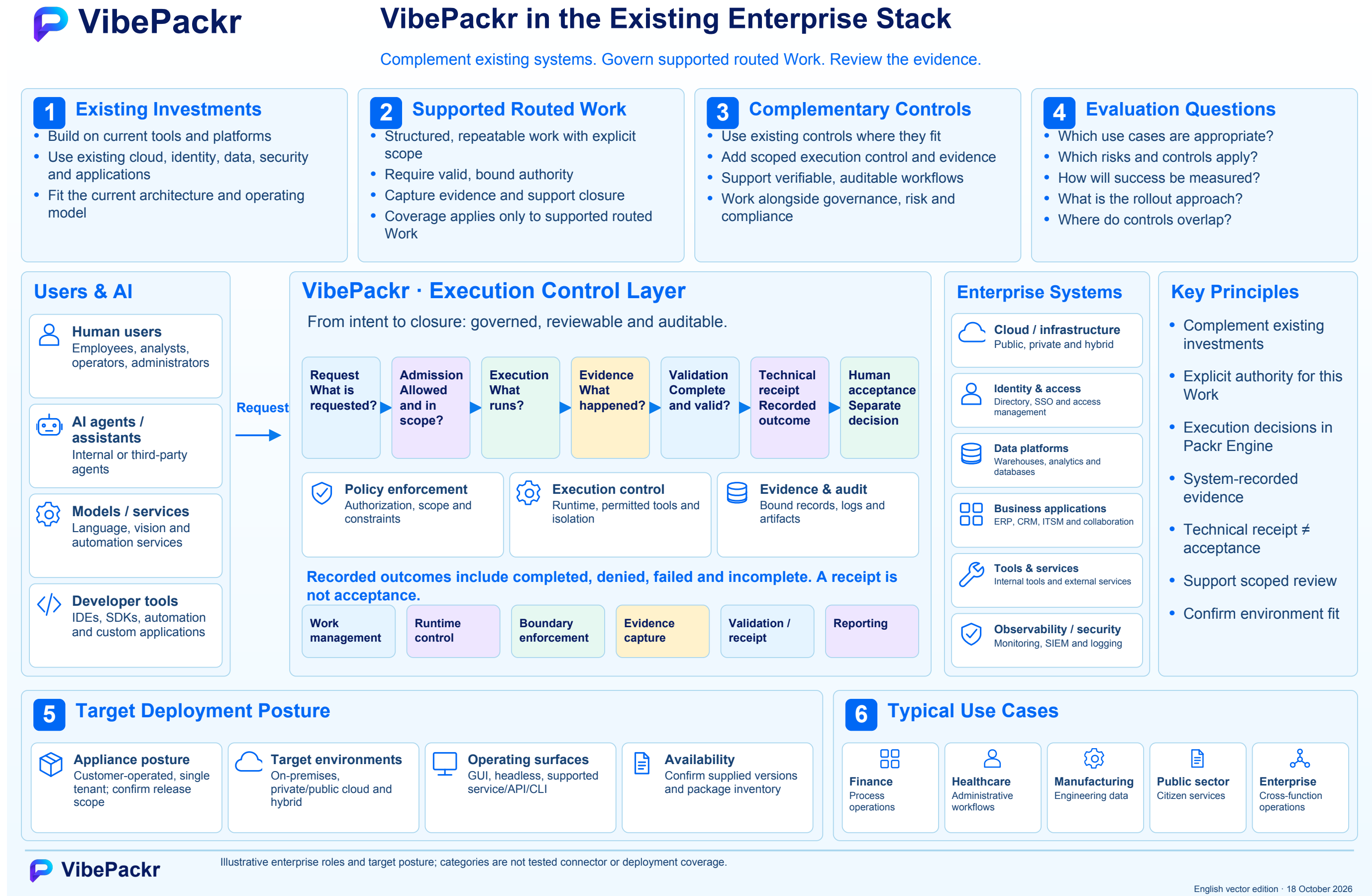


그림 29 · Non-SI 연동과 운영 적용



03 하나의 보호된 코어와 구분된 준비·Work 경로

기업 환경

권한이 부여된 시스템·데이터·인터페이스·정책·책임 소유자를 선택합니다. 맥락 분류는 호환성 목록이 아닙니다.

계약 및 문서 지원

기술적 선언은 의도·범위·제약을 담으며 검토된 자료는 Work 준비를 지원합니다. Document Supporter는 그 역할의 명칭이며 별도로 확정된 모듈이 아닙니다. 둘 다 권한을 부여하거나 법률 계약을 정책으로 해석하지 않습니다.

GAPE

Operator R1은 지정 범위의 Git/Rust/Tauri 정적 소스 탐색·대조·리비전 비교·오프라인 뷰어를 제공합니다. Headless는 제공된 스냅샷을 받고 GUI는 R0입니다. 이 서로 다른 인터페이스들은 권한을 부여하지 않습니다.

Integration Helper

R2는 정확한 GAPE 스냅샷과 독립적인 소유자·권한 바인딩을 바탕으로 아키텍처에 바인딩된 바인딩 및 검증 계획을 준비합니다. 메타데이터 후보도 GAPE의 참고가 될 수 있습니다. CLI 제출에는 등록 전송 경로가 없으며 준비는 바인딩이나 허가가 아닙니다.

SDK Engine

선택적으로 SDK Engine을 사용해 로컬 어댑터 후보를 만드세요. 전체 Enterprise 통합은 별도 구현·지원 범위이므로 Part.5와 해당 패키지에 제공된 요건을 따르세요.

Headless 및 사용자 인터페이스

Headless가 기본 운영 형태이며 PackrGUI는 사람의 요청과 검토를 위해 필요할 때 사용합니다. 관리·상태 인터페이스는 독립적으로 Work 권한을 소유하지 않습니다.

Work·증거·인수

보호된 Packr Engine이 지원되는 실행을 통제합니다. 검증·기술적 영수증·인수·종결은 서로 구별됩니다.

범위 및 한계

Packr Engine은 필요한 권한 확인을 거쳐 지원 Work를 통제·실행합니다. 준비 도구와 선택적 SDK 작성으로 입력·후보를 만든 뒤 연동 등록·검증을 완료하세요. 전체 Enterprise 통합은 별도 구현·지원 범위입니다.

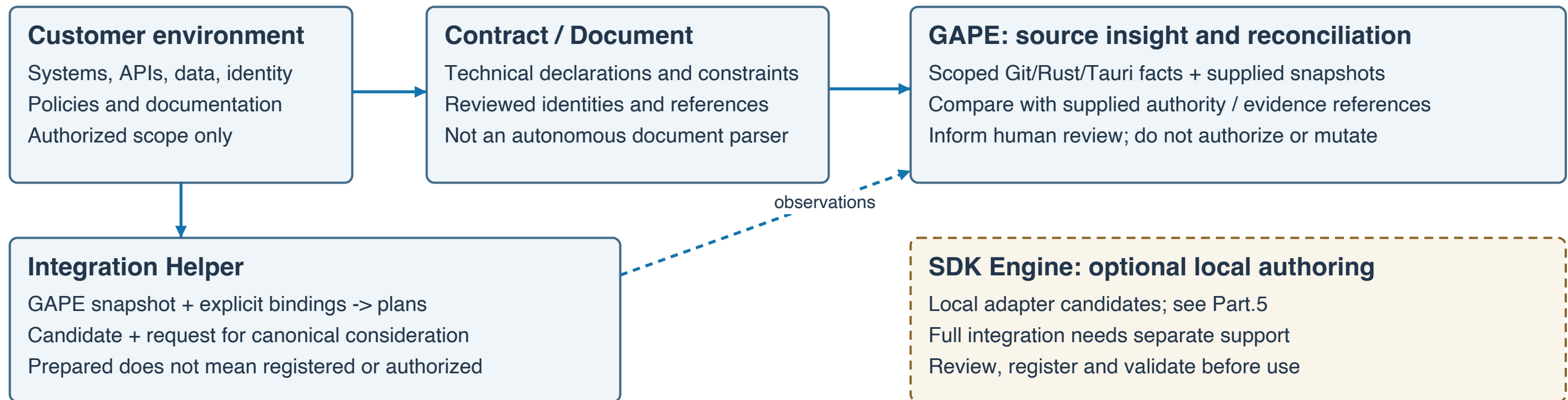
웹사이트에서 이어서 보기

</resources/system-overview/>

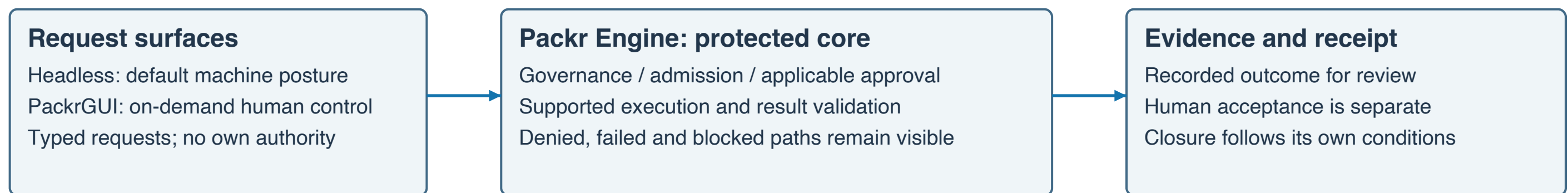
그림 2 · 기본 운영 모델

Enterprise operating model

Two related concerns: prepare understandable context; govern a supported Work. Not a mandatory linear pipeline.



SUPPORTED WORK PATH / protected governance and execution share the same core owner



Preparation handoff requests consideration only; no automatic bridge into live Work is asserted.

Admin scopes are distinct. Status is read-only. Review can inform new declarations and requests, not grant permission.

Solid arrows: bounded input / Work flow. Dashed arrow: observations, not automatic registration or execution.

그림 23 · 사람의 의도에서 통제된 Work까지



04 설치에서 운영까지: 필요한 도구 선택

Part.1~8과 같은 순서로 설치, GAPE 관찰, Integration Helper 준비, Contract·Document 선언, Helper 검증, 선택적 SDK·Builder 작성, 운영·검토를 진행합니다. 준비와 의사결정을 위한 흐름이며, 모든 Work에서 모든 도구를 실행해야 한다는 뜻은 아닙니다.

선언 전후의 Helper

선언 전에는 범위가 정해진 GAPE 스냅샷과 독립적인 바인딩을 바탕으로 Helper에서 요구사항·차이·담당자·검증 계획을 정리합니다. 선언 후에는 준비된 정확한 입력을 지원 Contract에 따라 검증하고 반환 사유를 인계에 반영합니다. 준비·등록·Work 바인딩·실행 권한은 별도 단계입니다.

SDK와 Builder를 생략할 수 있는 경우

기존 지원 인터페이스로 필요한 연결을 충족하면 새 SDK 작성을 생략할 수 있습니다. 기존 승인 Pack이 필요한 기능과 범위를 충족하면 Builder를 생략할 수 있습니다. 호환성·사용 자격·정책·Work 권한 검사는 계속 적용하며, 자산 재사용이 이전 실행 권한을 상속하지는 않습니다.

Online과 Offline은 모두 지원 선택지

대상 환경에 맞는 네트워크·의존성 경로를 선택합니다. Offline 의존성 세트는 폐쇄 온프레미스 준비를 위한 것이며 모든 배포의 기본값은 아닙니다. Online에서는 문서에 안내된 네트워크 사용 도구 체인을 이용할 수 있습니다. 어느 모드든 OS·아키텍처·패키지·네이티브 전제조건을 일치시킵니다.

웹사이트에서 이어서 보기

</docs/>

</docs/manuals/index.html>

</guides/on-premises/>

그림 32 · 설치와 도구 사용 흐름

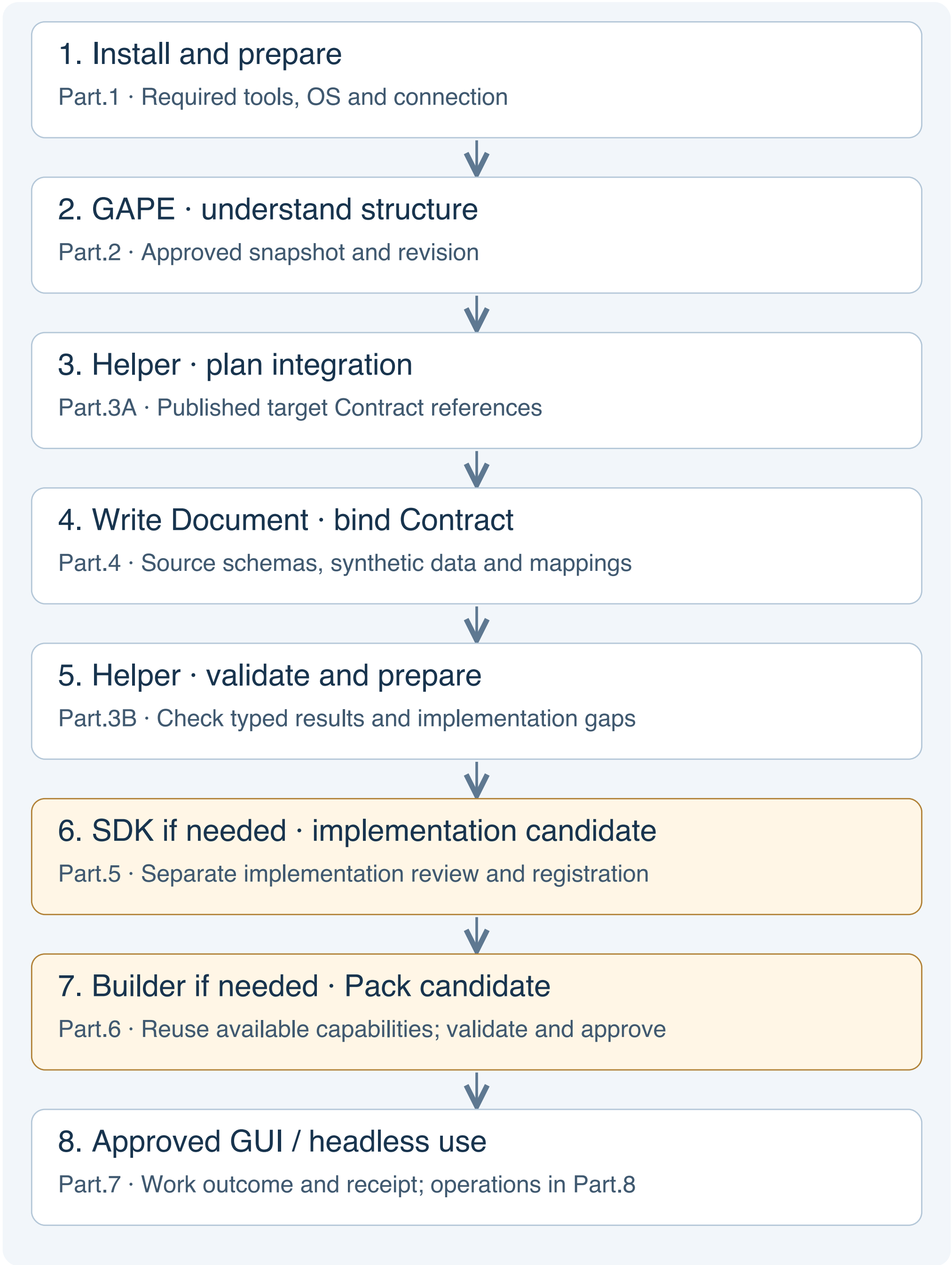
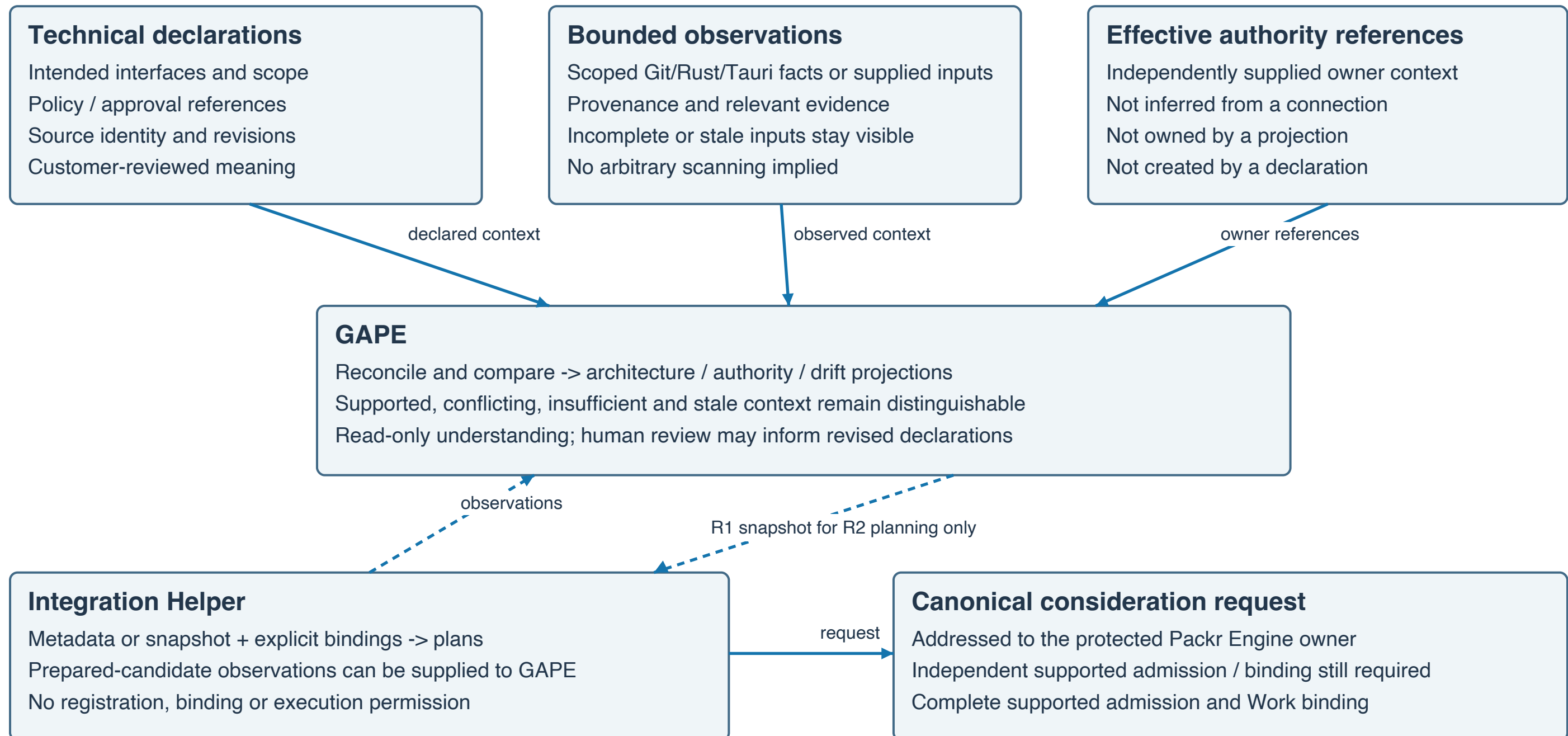


그림 3 · 선언과 준비

Declarations, observations and preparation

Inputs have different meanings. Reconciliation and candidate preparation do not create execution permission.



Declaration != discovery != preparation != registration != binding != authority != execution

05 GAPE: 소스 발견·대조·검토

권한이 부여된 입력

입력은 출처와 소스 사용 허가가 명시된, 범위와 리비전이 고정된 관찰 자료 및 참고 자료입니다. 계약·레지스트리·구성·런타임·증거·사용자 맥락은 소스 분류이며 범용 어댑터 목록이 아닙니다.

별도의 소스 탐색 작업

Operator R1은 명시된 범위의 커밋된 Git 블롭에서 제한된 정적 Rust 및 Tauri 등록·리터럴 호출 관계를 추출하고 리비전과 소스 출처를 보존합니다. 이 작업은 위 그림의 제공 입력 분기와 별개입니다. 정적 관계가 런타임의 실효성이나 권한을 입증하지는 않습니다.

대조

형식을 정규화하고 관련 사실을 연결하며 소유자를 매핑하고 리비전을 연결합니다. 충돌과 증거 누락을 조용히 사실로 바꾸지 말고 드러나게 유지해야 합니다.

정보 모델

중앙 모델은 구성요소·인터페이스·관계·소유자·출처를 기록합니다. 관찰 상태와 기대 상태를 구분합니다. 이 아키텍처 모델이 제품 실행 결정을 소유하지는 않습니다.

리비전 비교 및 오프라인 뷰어

R1에는 리비전 비교와 오프라인 HTML 검토 화면이 구현되어 있습니다. 그림 속 인터페이스는 개념도입니다. 내부 소스 상세와 허용 목록에 따른 공개용 투영은 서로 다른 출력이며, 그림이나 정제된 라벨만으로 공개 안전성이 입증되지는 않습니다.

두 가지 준비 관계, 활성화 없음

Helper는 후보 출처 정보를 관찰 자료로 제공할 수 있습니다. 별도로 Helper R2는 독립적인 제품·소유자·권한 바인딩과 함께 정확한 GAPE R1 스냅샷을 사용하여 계획을 준비합니다. 두 관계 모두 기능을 등록하거나 Work를 바인딩하거나 권한을 부여하지 않습니다.

범위 및 한계

운영자 탐색은 권한이 부여된 동결 Git 블롭과 제한된 Rust/Tauri 관계에 한정됩니다. Headless 검사는 새 스캔 없이 제공된 스냅샷을 사용하며, 현재 GUI 투영은 R0입니다. 범용 네트워크 탐색·완전한 런타임 적용 범위·실행 권한·자동 문제 해결을 의미하지 않습니다. 공유 전에 공개용 투영을 검토하십시오.

웹사이트에서 이어서 보기

</resources/gape-context/>

그림 4 · GAPE: 거버넌스 기반 아키텍처 프로젝트션



GAPE · Governed Architecture Projection Engine

Supplied, revision-bound observations. Source discovery is a separate operation.

ARCHITECTURE INSIGHTS FOR REAL-WORLD AI

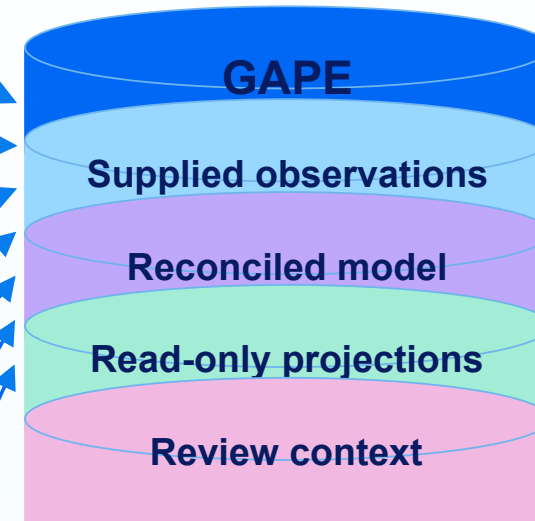
Reconcile supplied observations from authorized sources. Preserve provenance without changing the environment.

Same information. Better questions. Informed decisions.

Authorized Sources

- Architecture documents**
Designs, diagrams and standards
- Contracts / interfaces**
APIs, data models and integrations
- System / service records**
Configurations and inventories
- Existing assessments**
Reviews, findings and risk records
- Authority references**
Owners, teams and policy references
- Change history**
Commits, releases and artifacts
- Evidence and logs**
Audit records and test results

Reconcile multiple perspectives



Observed, candidate and reconciled facts remain distinguishable and bound to provenance.

Multiple Projections

- Architecture snapshot**
Observed/reconciled view at review time
- Authority projection**
Relevant owners and decision references
- Change analysis**
Observed revision differences
- Interactive exploration**
Read-only relationship review
- Reviewed projection**
Disclosure approval before external sharing

From supplied observations to informed review.

Facts can conflict.
Context matters.
People decide.

1 RECEIVE



- Collect supplied observations
- Authorized provided inputs
- Track revision and version
- Capture available evidence
- Inputs may be incomplete
- No scanning in this view

2 RECONCILE



- Normalize diverse inputs
- Unify data formats
- Resolve overlaps/conflicts
- Distinguish observed/candidate
- Link authority references
- Maintain traceability

3 PRESERVE PROVENANCE



- Build a source-bound model
- Components and interfaces
- Relationships and ownership
- Revision history
- No source mutation
- No execution authority

4 PROJECT



- Architecture snapshot
- Authority projection
- Change analysis
- Reviewed projection
- Derived, read-only views
- No automatic remediation

5 REVIEW



- Explore the relationships
- Components, interfaces, owners
- Changes and filters
- Confirm viewer availability
- Review before sharing
- Supports informed review

6 INFORM



- Understand architecture
- Identify review needs
- Spot drift and changes
- Support audit discussions
- Ask informed questions
- Human decisions remain separate

Design Objectives · evaluate in scope

Evidence with provenance

Governed by design

Revision drift awareness

Review risks before action

Enterprise context

Vendor-neutral inputs



GAPE reconciles supplied revision-bound inputs. It does not scan automatically, mutate the environment or authorize Work.

English vector edition · 18 October 2026

06 Integration Helper: 준비·검증·인계

준비 맥락 연결

Helper R2는 정확한 GAPE R1 스냅샷과 독립적인 제품·담당자·권한 바인딩을 사용합니다. 바인딩·검증 계획, 권한 대조, 차이 보고서, 공개 가능한 안내를 준비합니다. 알 수 없거나 지원되지 않는 바인딩은 준비 미완료로 유지합니다.

제공된 전체 요청 사용

제공된 요청을 새 실습 디렉터리에 복사합니다. 설치 버전에 맞게 문서의 `discover·normalize·validate·prepare·status` 명령을 실행하고, 각 단계의 표준 출력·표준 오류·프로세스 종료 코드를 보존합니다. 선언 발췌문은 설명용이며 지원되는 전체 요청을 대신하지 않습니다.

반환 사유에 따라 다음 조치

기록된 예제에는 DISCOVER PASSED와 CONTRACT_INCOMPATIBLE 사유의 NORMALIZE DENIED가 있습니다. 거절을 보존하고 정확한 필수 Contract와 요청 리비전을 확인합니다. Contract를 완화하거나 준비를 완료된 고객 연결로 표현하지 않습니다.

등록 승인과 연결은 별도로 완료

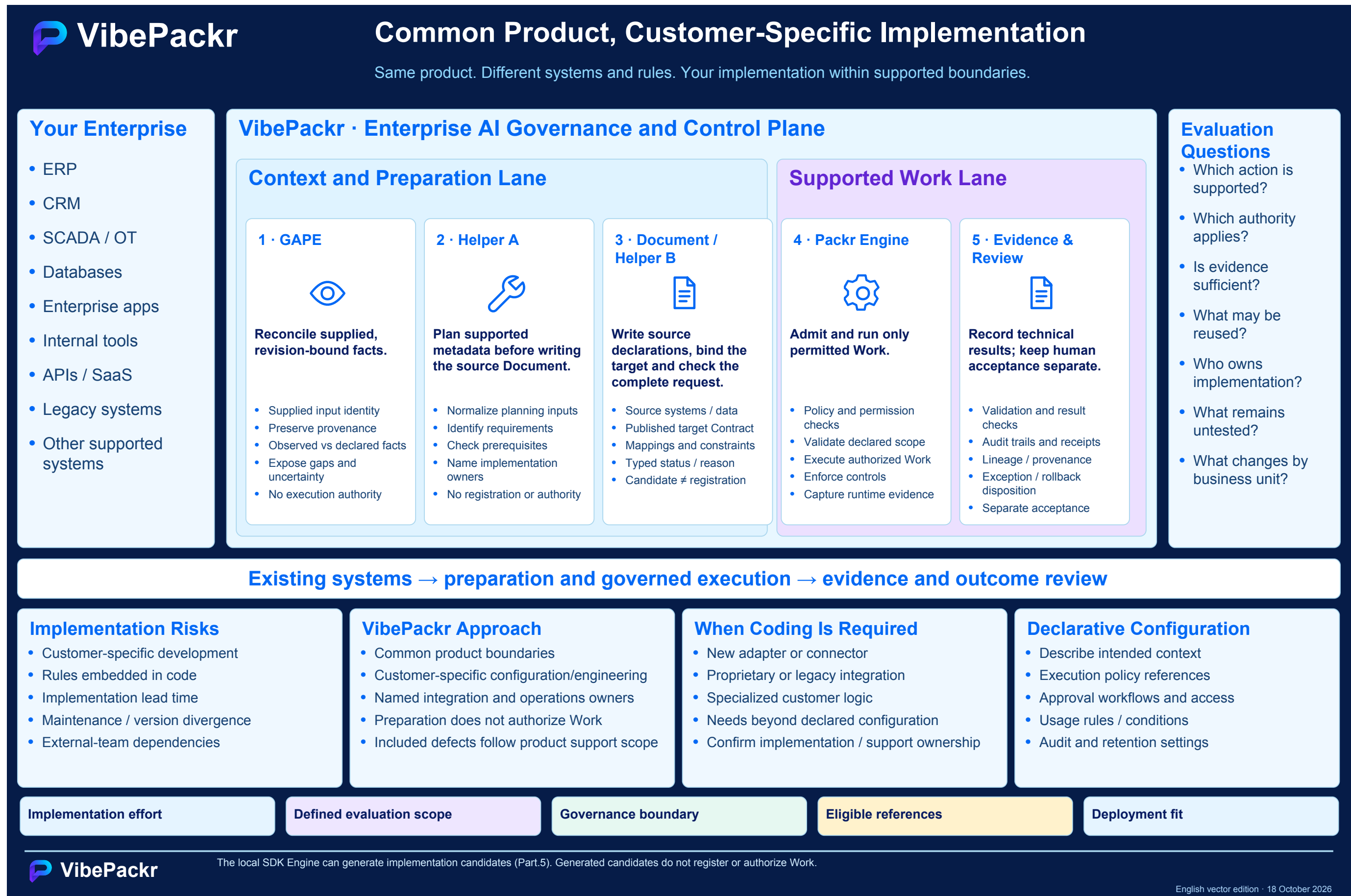
CLI 제출은 신뢰된 등록 전송을 제공하지 않습니다. 네이티브 레지스트리 등록 승인·Work 바인딩·필요한 실행 권한은 별도입니다. 생성된 골격은 구현이 필요하며, 대화 기록 픽스처는 로컬 시험 자료로서 실제 제공자 연결의 증거가 아닙니다.

웹사이트에서 이어서 보기

[/docs/manuals/Part_03_Integration_Helper.html](/docs/manuals/Part_03_Integration_Helper.html)

</guides/custom-execution/>

그림 17 · 공통 제품과 고객별 구현 책임



07 SDK Engine: 추가 권한 없는 확장

개발자 및 파트너 환경

다이아그램은 애플리케이션·데이터·개발 도구·기존 라이브러리·기업 시스템·문서에서 시작합니다. 이는 가능한 통합 입력이며 지원 언어나 커넥터 매트릭스가 아닙니다.

구현·통합·의존성

Part.5에 따라 로컬 SDK 어댑터 후보를 생성하세요. 지원 Rust 통합 API는 별도 인터페이스입니다. 후보를 다른 도구와 사용하기 전에 구현 검토·등록·연결 검증을 마치세요. 전체 Enterprise 통합과 데스크톱 임베딩에는 별도로 지원되는 구현이 필요하며, 기존 지원 Work 경로에서는 SDK 작성이 선택 사항입니다.

지원 계층

라이브러리와 인터페이스·패턴·시험 유틸리티·예제·버전 호환성·재사용 가능한 구성요소는 서로 다른 주제입니다. 참고 아키텍처는 모든 항목이 패키징되거나 출시되었다고 발표하지 않습니다.

확장 분류

사용자 정의 통합·애플리케이션·워크플로우 확장·도메인 확장·파트너 솔루션·재사용 모듈은 가능한 용도를 설명합니다. 확장 기능이 실행 권한을 이전하지는 않습니다.

탐색·개발·검증

선언된 인터페이스와 문서를 검토하고 사용 사례를 정한 뒤 지원 요건 안에서 구현하고 시험합니다. 호환성에는 증거가 필요하며 컴파일 성공만으로 충분하지 않습니다.

통합·준비·발전

선언된 인터페이스로 연결하고 구성을 문서화하며 호환성 매트릭스를 확인한 뒤 통제된 인계를 준비합니다. 이후 변경에도 호환성과 범위를 다시 검토해야 합니다.

범위 및 한계

SDK는 선택적으로 사용하는 작성 작업입니다. Part.5에 따라 로컬 후보를 생성한 뒤 지원 연결·등록·검증 단계를 완료하세요. 후보 생성만으로 Integration Helper·Headless·Packr Engine이 연결되거나 실행 권한이 부여되지는 않습니다.

웹사이트에서 이어서 보기

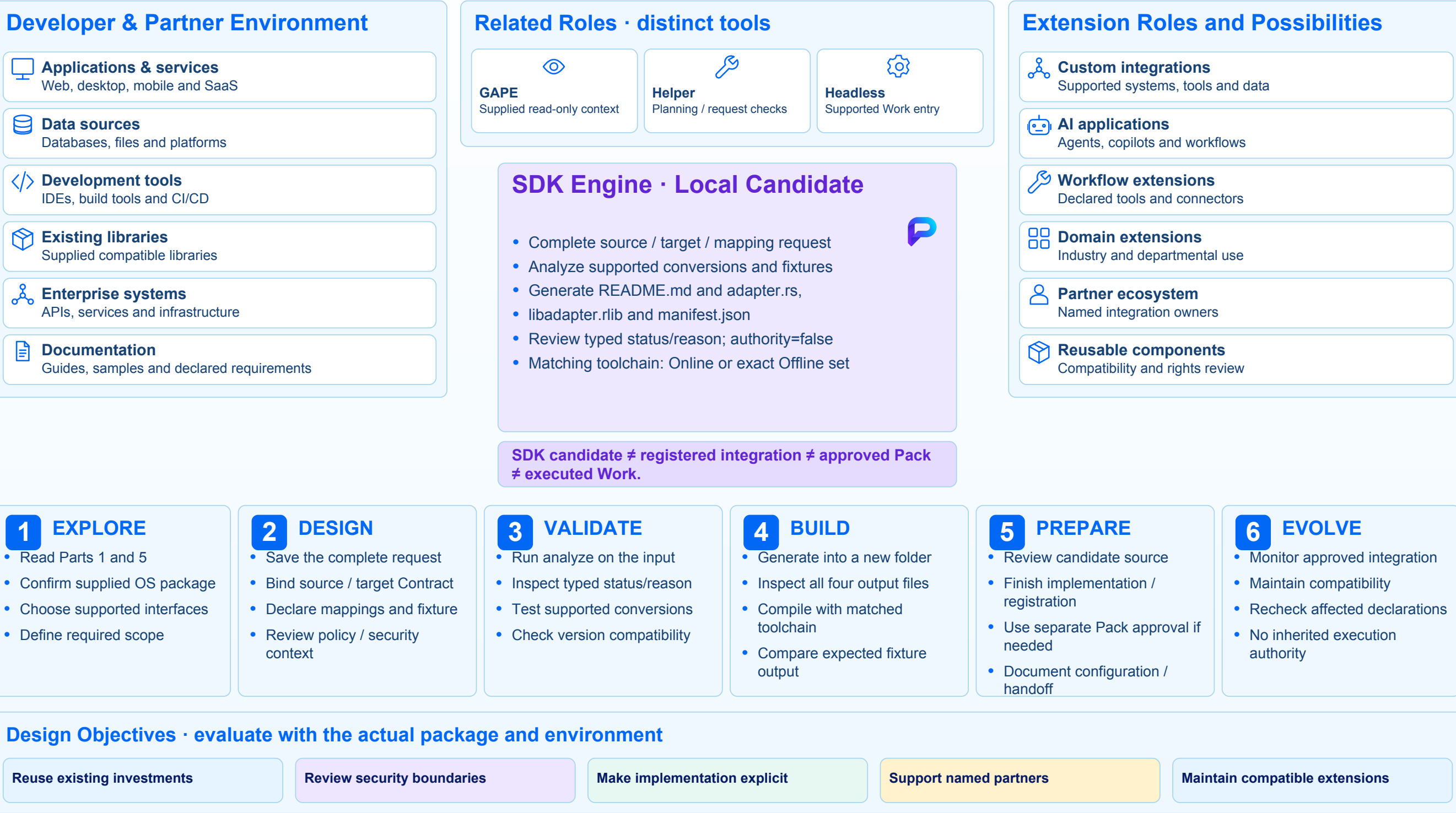
</resources/integration-extension/>

그림 20 · SDK Engine: 거버넌스를 유지하는 확장



SDK Engine · Extend with Governance

Local SDK candidate generation is available in the supplied SDK package. Registration and Work authority are separate.



08 로컬 SDK 예제: 입력·산출물·재현성

아래 설명용 발췌문이 아니라 패키지에 포함된 전체 읽기 전용 Custom API 요청으로 시작합니다. 로컬 픽스처는 component와 문자열 score를 반환하며, 매핑은 score를 정수 quality_score로 변환합니다. 이 실습은 로컬 후보 생성이며 실제 API 호출이 아닙니다.

JAVASCRIPT · 입력 수정

```
draft.fixture.response.score = "88"  
draft.fixture.response.component = "my-test-component"
```

score의 따옴표를 유지합니다. 같은 매핑의 논리적 기대값은 component="my-test-component", quality_score=88입니다. 명령은 이 매핑 객체를 실제 응답처럼 별도로 출력하지 않습니다. 따옴표 없는 숫자 score는 의도된 타입 오류 사례이며 정상 입력이 아닙니다.

새 디렉터리에서 네 산출물 확인

예상 파일은 adapter.rs·libadapter.rlib·README.md·manifest.json입니다. 소스와 매니페스트를 읽습니다. .rlib는 Rust 라이브러리이며 더블클릭해 실행하는 OS 응용프로그램이 아닙니다. 후보 상태는 CUSTOMER_REVIEW_CANDIDATE입니다. 매니페스트는 서명되지 않은 관찰 기록이며 릴리스 서명이나 독립적인 증명이 아닙니다.

같은 조건으로 비교

픽스처 값만 바꾸면 매핑 규칙이 같아 adapter.rs가 동일할 수 있습니다. 재현성은 같은 전체 입력·OS·SDK·컴파일러·의존성으로 다른 새 결과 디렉터리에서 확인하고 adapter.rs와 libadapter.rlib를 각각 비교합니다. 단계 결과와 의존성 트리 지문을 확인합니다. 전체 매니페스트 지문, 다른 OS 빌드, 다른 컴파일러 버전이 같을 것으로 가정하지 않습니다.

웹사이트에서 이어서 보기

[/docs/manuals/Part_05_SDK_Engine.html](/docs/manuals/Part_05_SDK_Engine.html)

09 헤드리스 운영과 사람의 검토 화면

Headless를 기본으로, 사람의 참여는 필요할 때.

지원 기계 요청과 형식화된 운영 질의는 그래픽 클라이언트를 계속 열어 둘 필요가 없습니다. 지원되고 범위가 정해진 Work만 통제된 실행 경로에 진입하며 보편적인 API·스케줄러를 주장하지 않습니다.

진입점 전반에서 하나의 판단 주체 유지

Headless는 타입이 정해진 요청을 제출하고 제품이 판단한 상태와 결과를 반환합니다. PackrGUI는 의도 입력·검토·인수를 위한 주문형 사람 인터페이스입니다. 화면을 이동해도 다른 권한 엔진이 생기거나 Work의 허용 범위가 달라지지 않습니다.

반환된 Work 확인

같은 Work 식별자를 상태·실행·검증·보고서 검토에 사용합니다. 서비스 실행 상태와 준비도는 다른 관찰이며, 명령 완료가 자동으로 Work 성공을 뜻하지 않고, 읽을 수 있는 보고서가 사람의 인수를 뜻하지도 않습니다. 설치 도구 사용은 Part.7, 기록 읽기 실습은 연결된 사례를 따릅니다.

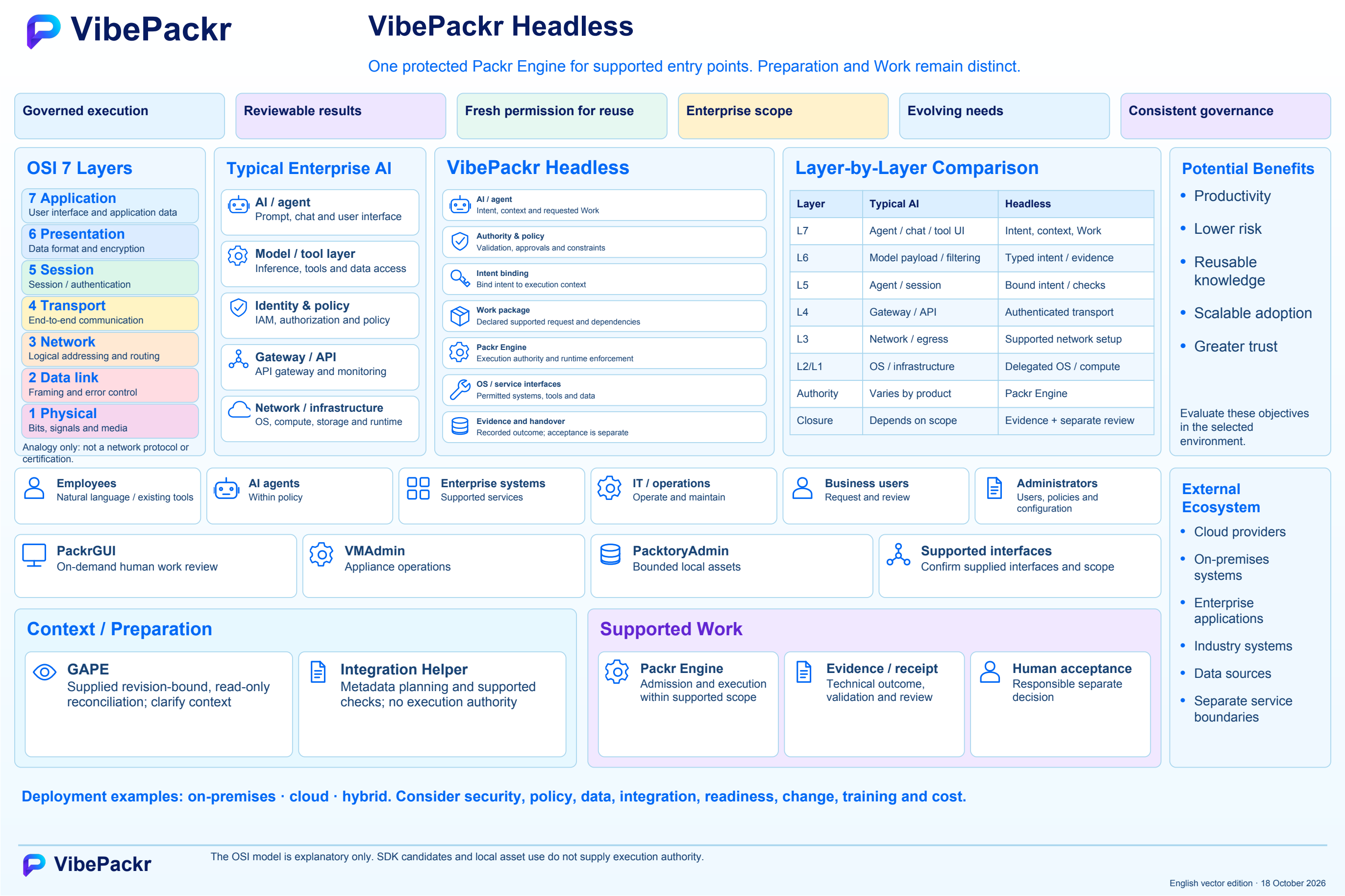
PacktoryAdmin·VMAdmin·읽기 전용 상태 화면은 선언된 관리·관찰 역할을 지원합니다. 제품이 판단한 결과를 사용하며 Work를 독립적으로 승인하지 않습니다.

웹사이트에서 이어서 보기

[/architecture/](#)

[/docs/manuals/Part_07_PackrGUI.html](#)

그림 6 · VibePackr 헤드리스 운영



10 통제된 실행: 요청에서 검토까지

1 · Work 요청

의도·목적·대상·범위·제약을 식별합니다. 요청은 실행 허가가 아니며 보고 예제는 설명용으로 ERP 호환성 증거가 아닙니다.

2 · 정책 및 맥락

ID·권리·분류·범위·전제조건을 적용 정책으로 평가합니다. 모델·도구 접근이 Work 권한을 부여하지 않습니다.

3 · 필요한 경우 승인

일부 Work에는 정책상 추가 승인이 필요합니다. 담당자·범위·조건을 기록합니다. 승인은 거버넌스 조건이며 정책을 대체하지 않습니다. 모든 Work에 승인이 필요한 것은 아닙니다.

4 · 통제된 실행

보호된 Packr Engine은 지원되며 권한이 부여된 경로를 통제합니다. 허용된 범위 안에서만 실행하며, 구체적인 격리 수준과 적용 범위는 평가가 필요합니다.

5 · 증거, 검증 및 영수증

관련 기록을 수집하고 선언된 기준에 따라 결과를 비교합니다. 증거와 검증은 불완전할 수 있습니다. 기술적 영수증은 결과를 기록하며, 업무상 인수나 자동 종결을 뜻하지 않습니다.

6 · 복구 및 계속 진행

문제가 생기면 중지하고 관련 증거를 보존합니다. 실패를 검토한 뒤 정책 범위에서 수정·재시도·상위 대응 요청 여부를 결정합니다. 복구는 통제된 결정이며 자동 재시작이 아닙니다.

7 · 재사용 및 Pack 지식

이전 결과는 권리·범위·적격성 검토를 거쳐야 재사용 후보의 참고 자료가 될 수 있습니다. 새 실행에는 새로운 권한이 필요하며, 성공한 Work가 자동으로 재사용 가능한 지식이 되지 않습니다.

8 · 보안 평가

선택한 범위에 적용되는 신원·접근·정책·격리·모니터링 통제를 평가합니다. 이 도식은 인증, 시험을 마친 보편적 적용 범위 또는 스케줄러 보장을 의미하지 않습니다. 다중 에이전트 Work에서는 공유 자원 위험을 별도로 평가합니다.

범위 및 한계

지원 연동 경로로 Work를 전달해 VibePackr의 실행 통제를 적용하세요. 다른 에이전트·도구·운영체제 동작에는 해당 플랫폼의 통제를 사용하세요. 기술적 영수증은 실행을 기록하며, 권한이 있는 검토자가 증거를 토대로 업무 인수·규제 준수·인증·법률 요건을 판단합니다.

웹사이트에서 이어서 보기

</resources/execution-boundaries/>

그림 7 · 요청에서 실제 실행까지



11 신원·접근과 Work Authority

LLM은 확률적으로 텍스트를 생성하며, 도구 실행 권한을 본질적으로 가져서는 안 됩니다. VibePackr는 다음을 엄격히 분리합니다: 제안 출처 권한. AI는 여러 접근법을 제안할 수 있지만 승인된 작업만 실행할 수 있습니다.

신원은 행위자를 확인하고 작업별 권한은 허용 동작을 정합니다.

세 가지 질문 구분

신원은 행위자를 식별합니다. 접근 권한은 해당 행위자가 이용할 수 있는 시스템·인터페이스를 정합니다. Work Authority는 요청한 특정 작업·대상·범위·적용 조건을 다룹니다. 로그인 성공이나 API 토큰이 모든 Work 권한 질문에 답하지는 않습니다.

정확한 요청에 승인 연결

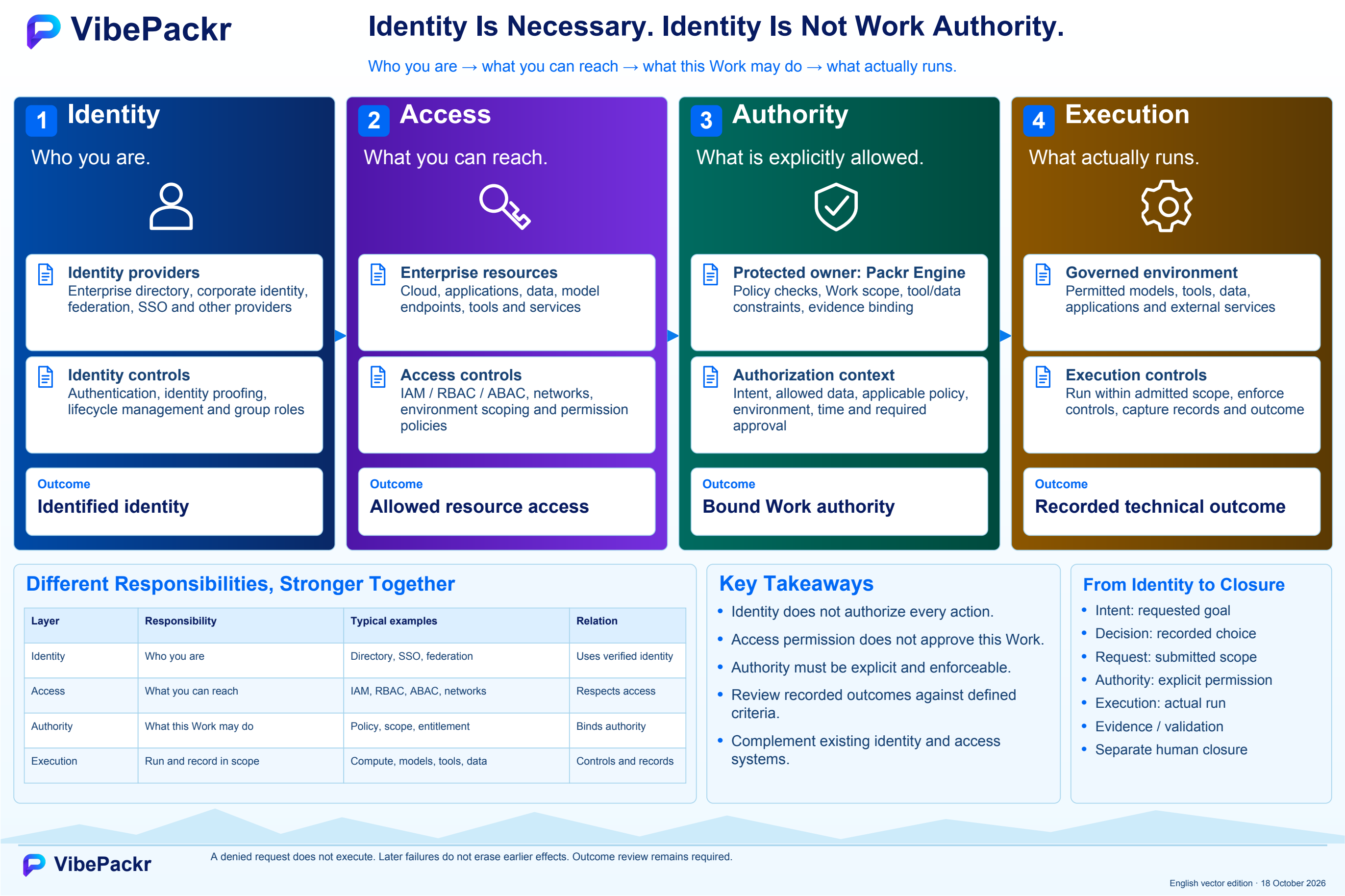
정책상 승인이 필요하면 해당 작업과 현재 조건을 지정한 결정인지 확인합니다. 이전 승인·재사용 Pack·사용 가능한 도구가 새 대상을 승인하지는 않습니다. 거절은 해당 요청의 종료 결과이며, 조용히 다음으로 진행하는 성공 단계가 아닙니다.

웹사이트에서 이어서 보기

</howto/>

</resources/enterprise-ecosystem/>

그림 8 · 신원·접근과 Work Authority의 구분



12 증거를 통한 검토와 책임 있는 인수

“또 하나의 대시보드가 아닌, 시스템이 입증할 수 있는 상태의 투영.” 기업 이해관계자의 서로 다른 보증 관점으로 하나의 통제된 업무 기록을 표시합니다.

통제된 Work 수명주기

사용자 또는 자동 요청을 수집하고 범위를 정해 구조화된 작업 의도로 정규화합니다. 요청 수집은 실행 승인이 아닙니다.

하나의 Work 기록, 여러 보증 관점

통제된 Work 기록은 서로 다른 검토 질문을 지원합니다. 관찰·증거·검증·영수증·인수·종결은 구분되며 기술적 영수증은 사람이나 업무의 인수가 아닙니다.

관찰·검증·인수

로그·상태는 관찰을 설명합니다. 증거는 관련 기록·산출물을 보존합니다. 검증은 관찰 결과를 명시된 기준과 대조합니다. 기술 리시트는 기술적 처리 결과를 기록합니다. 책임 검토자는 그 뒤 업무 결과를 인수·보류·거절할지 판단합니다.

식별자와 미완료 증거 보존

결과를 비교하기 전에 Work·리비전·입력·산출물 식별자를 일치시킵니다. 빠진 검사는 누락으로 기록하며 파일 존재나 해시 비교 성공을 업무 내용의 정확성으로 확대하지 않습니다. 수리는 연결된 새 결과를 만들고 실패 시도는 기록에 남습니다.

웹사이트에서 이어서 보기

</architecture/>

</docs/packrgui-final-report-en.html>

그림 9 · 관찰·증거·검증·인수



Observability, Evidence, Validation and Acceptance

Different questions. Bounded conclusions. Responsible decisions.

1 Observability

What did we observe?

- Application logs
- Traces, telemetry, metrics
- Events and audit logs
- Network and infrastructure
- Security signals

- Visibility and monitoring
- Operational insight
- May lack context
- Does not verify correctness

2 Evidence

What supports the claim?

- Execution logs
- Relevant input/output data
- Tool/component calls
- Files, changes and manifests
- Execution metadata / artifacts

- Preserve and bind data
- Link identity, time and context
- May be incomplete
- Evidence alone is insufficient

3 Validation

Does evidence meet criteria?

- Identity / authority checks
- Hash/signature integrity
- Scope and policy checks
- Expected vs actual comparison
- Completeness and environment

- Evaluate declared criteria
- Use available evidence
- Additional analysis may apply
- No unlimited guarantee

Technical Receipt

System record of the scoped outcome.

Identity and evidence references.

May be denied, failed or incomplete.

Not acceptance.

4 Acceptance and Closure

Can this Work be accepted?

- Responsible human owner
- Accountable reviewer
- Decision and rationale
- Closure record / audit package
- AI / systems: information only

- Human authority owns acceptance
- Defined criteria and ownership
- Further review may be required
- No automatic acceptance

Comparison at a Glance

Aspect	Observation	Evidence	Validation	Receipt	Acceptance
Question	What happened?	What is shown?	Criteria met?	What was recorded?	Accept complete?
Records	Logs / traces	Related artifacts	Validation record	Execution record	Decision record
Scope	Activity / signals	Selected data	Defined criteria	Executed scope	Work context
Integrity	May change	Bound records	Criteria-bound	Identity-bound	Own rationale
Owner	Operations	Data / compliance	Validation role	System	Human owner
Boundary	Not proof	Not sufficient	Bounded checks	Not acceptance	Human decision

Key Takeaways

- Observation shows activity.
- Evidence preserves what can be shown.
- Validation evaluates the claim.
- A receipt records technical outcome.
- Acceptance and closure are human decisions.
- Evaluate evidence quality and usefulness.

From Signals to Reviewable Trust

A governed path requires more than monitoring or logs.

Inspect relevant records, defined criteria, limits and accountable review.



Record integrity does not establish truth or completeness. Claim strength must follow the available evidence.

English vector edition · 18 October 2026

13 기업 AI 도입·사용의 규제 감사 검토

Governed Work Execution Control Plane은 지원되는 AI Work에 Work Authority(업무 실행 권한)·정책·범위를 적용합니다. 기업 AI 도입·사용의 규제 감사 검토에서 권한 판단, 실행 또는 거절, 검증, 증거, 기술 리시트를 추적할 수 있습니다.

검토 가능한 연결 기록 구성

의도한 사용 목적과 업무 책임자에서 시작합니다. 지원 실행 경로·허용 신원과 데이터 범위·적용 정책·필요 승인을 식별합니다. 관찰된 실행 또는 거절을 선택한 Work·검증 결과·보존 산출물에 연결합니다. 검토자가 전체 과정에서 같은 식별자와 리비전을 확인하도록 합니다.

실제 사용에 의무 매핑

조직과 사용 사례에 적용되는 요구사항은 법무·보안·위험 담당자가 판단합니다. 각 적용 요건에 통제·담당자·확인할 증거·남은 차이를 대응시킵니다. 제품 다이어그램·로그·기술 리시트 하나만으로 준수나 인수가 성립하지는 않습니다.

결론은 책임 조직에서 판단

실행 증거는 기업 AI 도입·사용 검토를 지원합니다. 최종 준수·인수 판단은 책임 조직에 있습니다. 이 백서는 기술 설명과 평가 경로를 제공하며 준수를 인증하거나 감사 결과를 보장하거나 법적 시한을 정하지 않습니다.

웹사이트에서 이어서 보기

[/#enterprise-knowledge](#)

[/resources/evaluation-path/](#)

[/guides/poc/](#)

14 고객·VibePackr·제3자의 책임

고객의 목표·데이터·정책

고객은 업무 목표와 성공 기준을 정하고 데이터 권리를 확보하며 조직 정책·권한·허용 용도를 승인합니다. 데이터가 있다는 사실만으로 처리 권한이 부여되지는 않습니다.

고객의 모델 선택 및 결정

모델·공급업체 선택, 결과 해석, 최종 업무 결정은 고객의 책임으로 남습니다. 실행 기록이 모델 답변의 진실성을 인증하지는 않습니다.

통합·운영·도입

고객과 지정된 구현 담당자는 합의된 범위에서 고객별 어댑터·마이그레이션·워크플로우 설계·운영 전환·인프라 운영·데이터 권리·접근·교육을 담당합니다. 제품화된 지원이 해당 프로젝트를 맡지는 않습니다.

VibePackr 제품 경계

보호된 코어는 지원되는 Work와 증거를 통제합니다. 관리는 클라이언트 역할이며 Headless 어플라이언스 내부에 필요한 GUI가 아닙니다. 포함된 제품의 결함은 적용되는 지원 범위에 남으며, Non-SI가 모든 통합 관련 제품 결함을 제외하지는 않습니다.

제3자 서비스 및 인프라

모델·클라우드·소프트웨어 공급업체는 각자의 조건에 따라 운영합니다. 예시는 제휴·보증·시험된 통합을 의미하지 않습니다.

관할 기관·생태계·콘텐츠 소유자

적용 법률·외부 표준·콘텐츠 권리는 제품 통제와 별개입니다. ISO·NIST·HIPAA의 언급은 인증이나 규정 준수 주장이 아닙니다.

법률 문서와 함께 읽기

이 역할 지도는 설명용입니다. 실제 책임은 적용 법률과 체결된 계약을 따릅니다. 공개된 지원 SLA는 법률 검토가 필요한 초안입니다.

범위 및 한계

실행 통제가 모델 정확성·업무적 정확성·규제 준수·제3자 가용성을 보장하지는 않습니다. 책임은 적용 계약과 법률을 따르며 공개 SLA는 법률 검토가 필요한 초안입니다. 고객의 모든 프로젝트가 아니라 경계를 표준화합니다. 그림은 지원 약속을 만들거나 고객 운영을 VibePackr로 이전하지 않습니다.

웹사이트에서 이어서 보기

</resources/shared-responsibility/>

그림 10 · 역할별 공동 책임



Who Is Responsible for What?

Clear roles. Shared responsibility. Product execution control and customer decisions remain distinct.

Customer

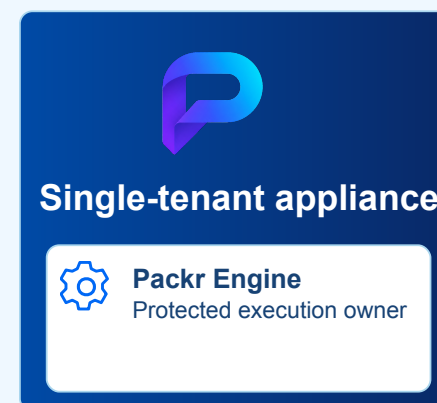
Own your business, data and decisions

- Business objectives**
Define goals, use cases and success criteria.
- Data ownership & rights**
Confirm legal rights, accuracy and appropriate use.
- Policy & governance**
Approve internal policies, permissions and acceptable use.
- Model selection & use**
Choose and configure models/providers for requirements.
- Business decisions**
Interpret results and make business decisions.
- Integration projects**
Implement customer-specific integrations using supported tooling; name the owner.
- Operating environment**
Manage infrastructure, network, access, security and backup.
- Training & adoption**
Train users and establish operating procedures.

VibePackr

Governed execution for supported Work

Product governance, control and evidence within supported scope. Clients have no independent execution authority.



Helper
Preparation

GAPE
Reconciliation

Separate client interfaces: PackrGUI · VMAdmin · PacktoryAdmin

Third Parties

External services you engage

- AI model providers**
Their model service behavior, availability and outputs.
- Cloud infrastructure**
Their compute, storage, network and platform services.
- Software / integration providers**
Their software, APIs, connectors and external systems.
- Regulators / authorities**
Applicable law and requirements within their authority.
- Industry / ecosystem**
Industry frameworks, standards and practices.
- Content owners**
Rights and usage terms for external data and knowledge.

Key Takeaways

- Clear roles**
Responsibility supports trust and adoption.
- Product execution controls**
Controls supported Work; acceptance remains separate.
- You remain responsible**
Your data, policies and business decisions.
- Complementary ecosystem**
Each party owns its service and obligations.



Explanatory role map. Executed agreements, product support scope and applicable law define actual responsibilities.

English vector edition · 18 October 2026

15 배포·복구: 계산 자원·저장·검증

배포 토폴로지

목표는 고객이 통제하는 단일 테넌트 Headless VM 어플라이언스와 별도의 사용자·관리 클라이언트입니다. 컴퓨팅·영속 시스템 및 증거 데이터·시험된 백업은 서로 다른 주제입니다. 미래의 호스팅 저장소가 현재의 원격 서비스를 뜻하지는 않습니다.

재개 전 준비 상태

자원 환경·신원·접근·런타임·정책·범위를 확인한 뒤 준비 상태를 검증합니다. SDK Engine은 선행 조건이 아닙니다. 컴퓨팅 복원이 준비 완료로 뜻하지 않으며 준비 완료가 Work를 승인하지도 않습니다.

일시적 중단

재시작 경로에서는 런타임 재시작·상태 확인·구성과 신원 확인·연결 재수립을 수행하고 작업 재개 전에 검증해야 합니다.

VM 교체

교체 경로에서는 호환되는 컴퓨팅 환경·복원되거나 재바인딩된 구성·온전한 영속 저장소와의 재연결·접근 및 신원 검사·의도된 동작 검증이 필요합니다.

컴퓨팅은 저장소가 아니며 저장소는 백업이 아닙니다

교체 가능한 VM이 데이터 보존을 보장하지는 않습니다. 복구는 온전한 데이터·사용 가능한 자격 증명과 키·호환 버전·보존 결정·시험된 복원 절차에 달려 있습니다.

자원 및 플랫폼 가정

통제 계층의 자원 요구는 모델 추론 하드웨어와 별개입니다. 배포 대상·용량 산정·복구 절차는 해당 평가와 릴리스에 맞게 확인해야 합니다.

평가 목표이며 서비스 약속이 아닙니다

하단 패널은 평가와 향후 운영의 목표입니다. 측정된 이점·복구 시간 목표·복구 시점 목표·가동 시간 약속·무손실 보장 이 아닙니다.

범위 및 한계

해당 릴리스에 제공된 배포·복구 절차를 따르세요. 복구 시간·복구 시점·데이터 손실·가동 시간의 약정은 이 다이어그램이 아니라 적용 계약을 기준으로 확인하세요. SDK 작성은 선택 사항이며 설치·복구와 별개입니다. 컴퓨팅 복원 후 준비 상태를 검증하고 재개 권한을 확인한 뒤 Work를 다시 시작하세요.

웹사이트에서 이어서 보기

</resources/recovery-boundaries/>

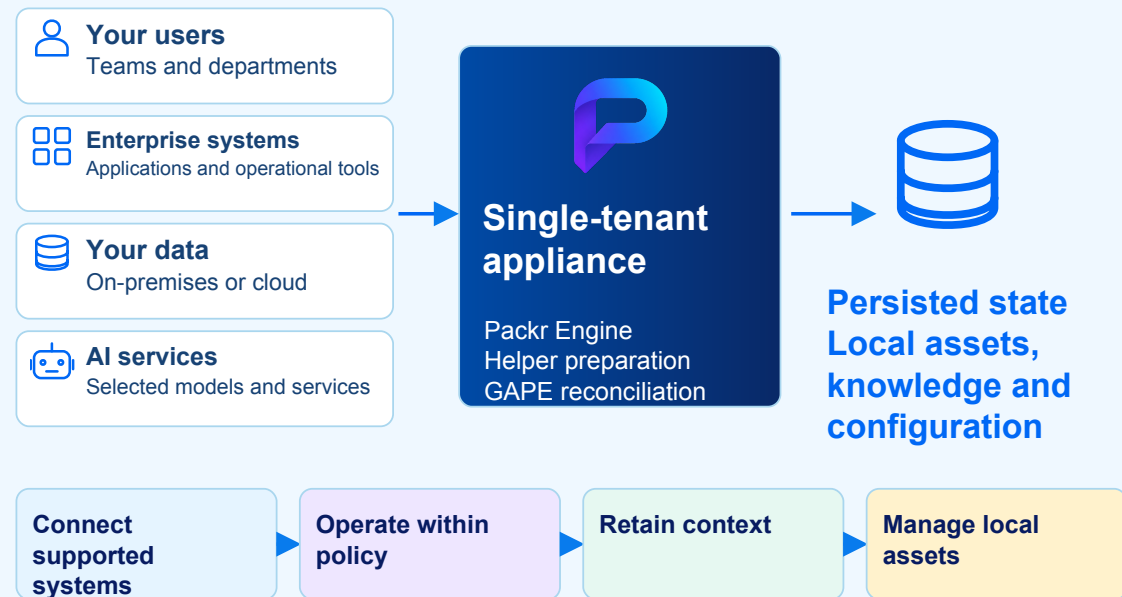
그림 11 · 운영과 복구



Operating Model & Recovery

Recover state and authority. Validate before resumption. Recovery is conditional.

1 Normal Operation



2 When a VM Issue Occurs



Example: temporary issue

- Restart the VM where appropriate
- Verify system health
- Confirm configuration and identity
- Reconnect required systems/services
- Resume only after validation

No automatic or guaranteed restoration.

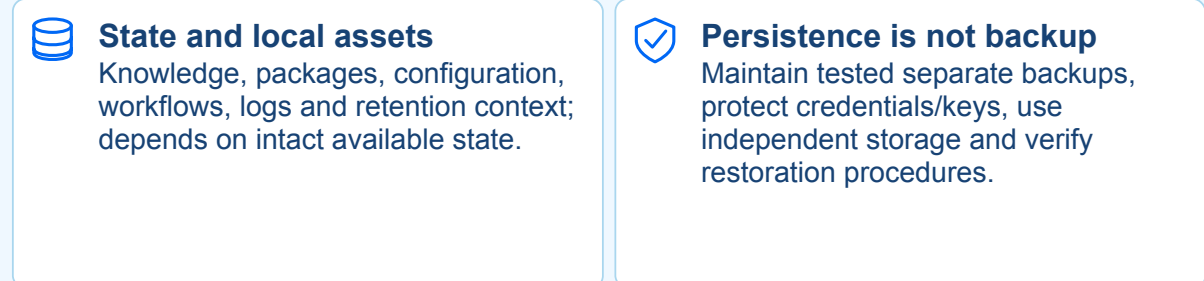
3 If the VM Is Damaged



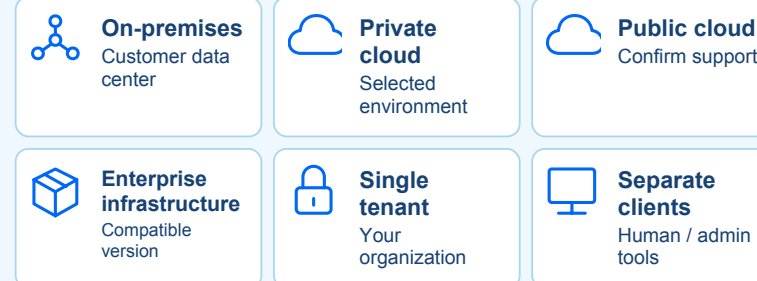
Example: VM replacement

- Deploy compatible compute and release
- Restore/rebind configuration and identity
- Reconnect available persisted state
- Verify systems, dependencies and access
- Validate before resuming

Persistent State and Dependencies



Operating Environment



Operational Considerations

- Monitoring, logging and alerting
- Clear upgrade / replacement route
- Existing backup strategy
- Security and retention policy
- No RTO, RPO or zero-loss promise

Key Takeaway

Recover state and authority. Validate before resumption.

Requires compatible compute and versions, intact state, tested backups, credentials/keys, valid authority and successful validation.



Fresh VM findings do not authorize changes to the frozen Golden image. Remote Rescue transport remains disabled.

English vector edition · 18 October 2026

16 Packtory: 상세한 향후 지식 아키텍처

위치와 작업-참조 순환

이 개념은 의도 해석·통제된 실행·지식 저장·기업 환경을 연결합니다. 검토된 작업은 이후 요청에 참고가 될 수 있으나 실행 허가를 이전하지는 않습니다. Headless 라벨은 운영 인터페이스를 나타내며 두 번째 보호된 권한 또는 실행 엔진을 뜻하지 않습니다.

제안된 기능

이 개념에는 패키징·메타데이터·계보·버전 관리·분류·검색·적응·공유가 나열됩니다. 제안된 호스팅·공유 역할은 현재의 서비스 목록이 아닙니다.

Pack 유형 예시

Work·보고서·데이터셋·프로세스·모델·솔루션·훈련·참고 Pack은 서로 다른 지식 형태를 예시합니다. 라벨이 처리 권리나 운영 적격성을 입증하지는 않습니다.

접근 분류

내부·고객 범위·공개 공유는 개념적 분류입니다. 저장·처리·재배포 권리는 별도로 평가해야 하며 공유가 실행 권한을 부여하지는 않습니다.

제안된 서비스 아키텍처

저장·버전 관리·정보 보강·분류·검색·참고 자료 처리·접근이 개념적 서비스를 구성합니다. 외부 신원·협업·저장소 통합이 제공된다고 주장하지 않습니다.

수명주기 및 검토

수집·정보 보강·분류·패키징·저장·검토·재사용·피드백은 개념적 단계입니다. 재사용 전에 검토해야 하며, 저장된 산출물이 자동으로 적격해지지는 않습니다.

재사용 적격성

정책·권리·민감도·출처·범위·사람의 검토가 적격성을 결정합니다. 이전 작업의 성공을 근거로 불명확하거나 누락된 권리를 추론할 수 없습니다.

예시 및 목표

그림의 분류가 고객 작업 수집을 승인하지는 않습니다. 권리·민감도·범위·적격성은 독립적인 검토가 필요합니다. 제한된 로컬 Packtory는 미래의 호스팅·공유 서비스와 구별되며, 원격 Rescue 전송은 비활성 상태입니다.

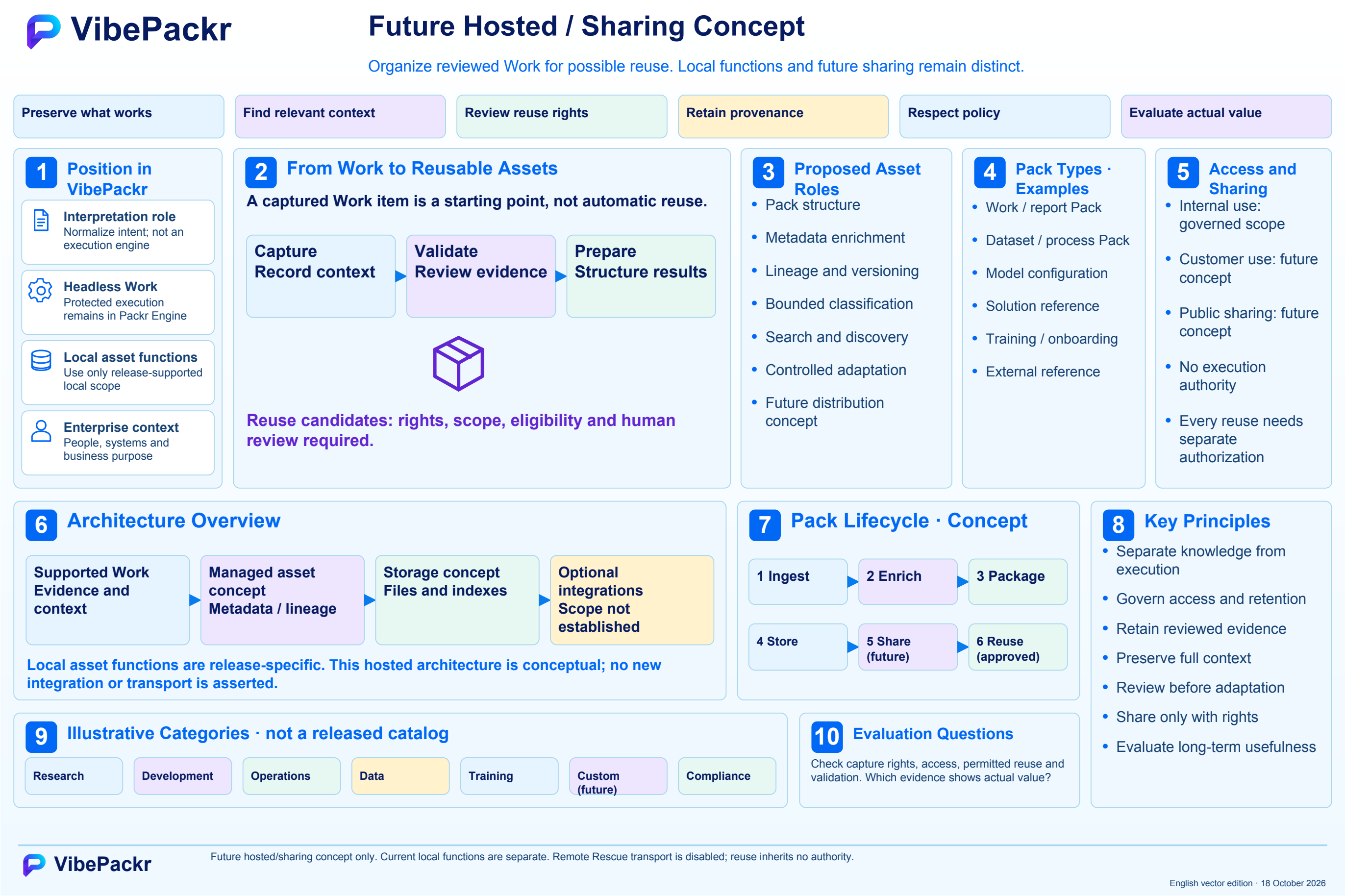
범위 및 한계

미래의 호스팅·공유 개념은 제한된 로컬 Packtory와 구별됩니다. 고객 작업의 무제한 업로드나 공유를 제공하지 않으며 원격 Rescue 전송은 비활성 상태입니다. 재사용이 실행 권한을 이전하지는 않습니다.

웹사이트에서 이어서 보기

</resources/knowledge-concept/>

그림 12 · 향후 호스팅·공유 구상



17 기업 평가: 확장 전에 의존성 확인

1 · 기존 AI 플랫폼이 있는 경우

기존 플랫폼과 함께 한정된 실행 통제 계층을 검토합니다. 기존 데이터 연동·의사결정 지원이 새 Work 요청을 허가하지 않습니다. 잠재 이점은 평가할 가설입니다.

2 · 기존 기업 스택의 거버넌스 공백

기존 시스템에서 유용한 흐름 하나를 선택합니다. 지원 인터페이스·버전·권리·구현 책임자를 확인하십시오. 도해는 보편적 연동이나 교체 없는 프로젝트를 약속하지 않습니다.

3 · 규제 또는 보증 요구

결정에 필요한 검토 기준·배포 제약·증거를 정의합니다. 실행 통제는 한정된 검토를 돕지만 준수 인증이나 책임 있는 판단을 대체하지 않습니다.

생태계 적합성 평가

클라우드·데이터·ID·앱·모델·자동화는 설명용 맥락 분류이며 시험된 커넥터 목록이 아닙니다. 정확한 지원 환경·연동 범위를 확인합니다.

확장 전 테스트

담당자·허용 입력·실행 허용 조건·결과 기준을 합의합니다. 의도한 경로뿐 아니라 거부·누락 전제조건·검사 실패·불완전 증거도 평가합니다. 확대 도입에는 별도 준비·인수 결정이 필요합니다.

조건부 확장이며 필수 파이프라인이 아님

지원 연결 경로부터 확인하세요. 새 어댑터가 필요하면 구현 담당자를 정하고 Part.5의 로컬 SDK 작성과 호환성 검증을 진행하세요. 업무에 필요한 경우에만 확장을 추가하고 전달 범위·일정은 별도로 합의하세요.

범위 및 한계

이 다이어그램으로 필요한 선택적 확장을 계획하세요. Part.5는 로컬 SDK 작성을 안내하며 전체 Enterprise 통합에는 별도 구현과 검증이 필요합니다. 배포 전에 적용 범위·지원·인수 기준을 합의하세요.

웹사이트에서 이어서 보기

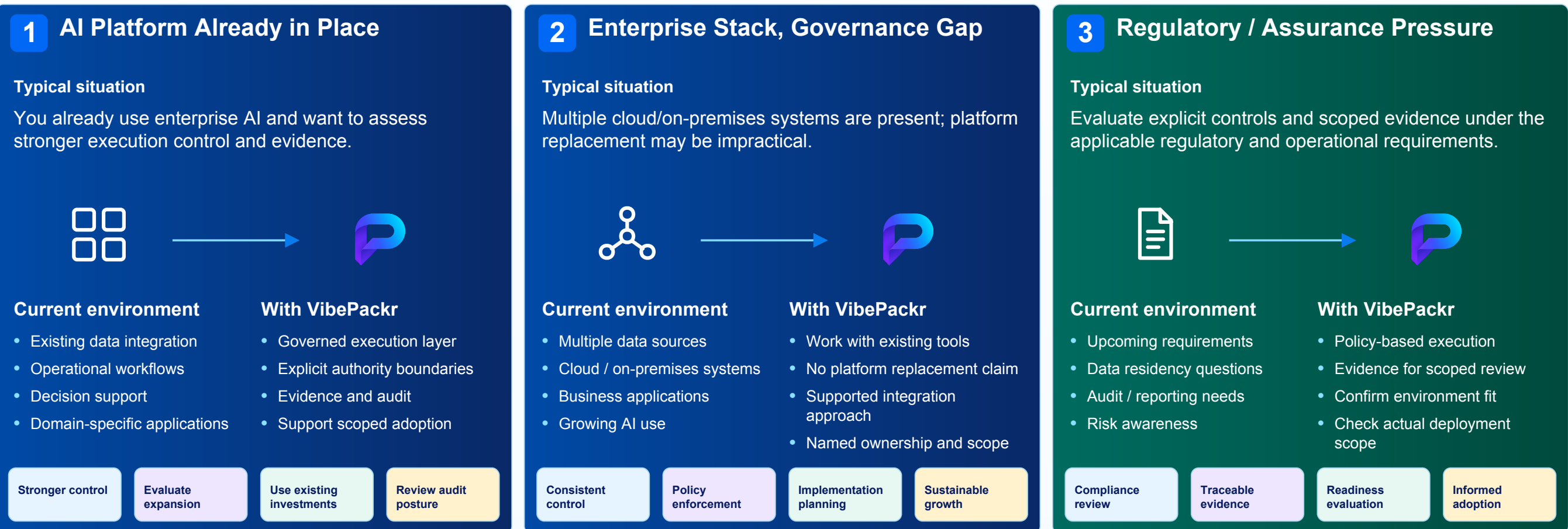
</resources/evaluation-path/>

그림 13 · 다른 출발점에서 시작하는 평가



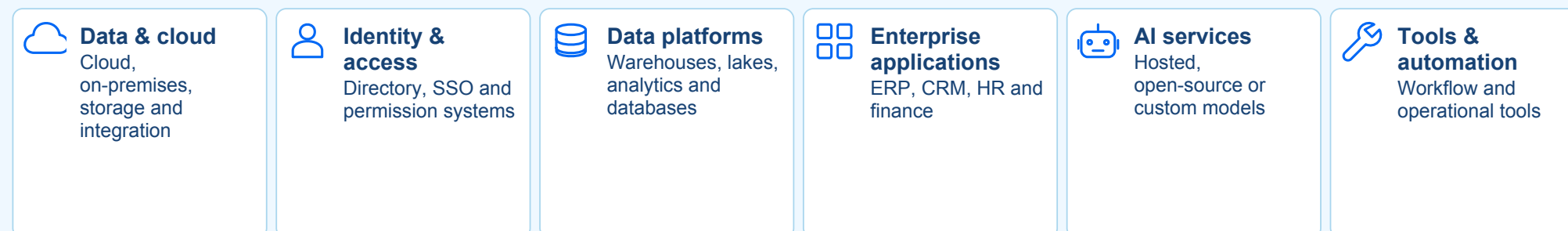
Different Starting Points. A More Reliable Future.

Illustrative evaluation scenarios, not customer case studies or promised deployment outcomes.



Evaluate Fit with Your Enterprise Ecosystem

Confirm supported interfaces, versions and scope. These categories are not a tested connector list.



One Principle Across Scenarios

- Complement existing investments
- Explicit Work-specific authority
- Bounded evidence for review
- Confirm environment fit
- No implied compliance certification



No fixed timeline, customer outcome or compatibility guarantee. Evaluate the actual selected environment and supplied product scope.

English vector edition · 18 October 2026

18 빙산: 실행 아키텍처의 네 계층

보이는 표면

빙산은 계층 비유이며 현재의 주요 운영 모델이 아닙니다. Headless가 기본 운영 형태이며 PackrGUI는 필요할 때 사용하는 사람의 요청·검토 클라이언트입니다. 관리와 상태는 각각 별도 범위이며 독립적인 Work 권한이 없습니다.

기능 계층

터미널 작업에는 Headless를, 정해진 읽기 전용 검토에는 GAPE를, 준비에는 Integration Helper를, 지원 자산 관리에는 로컬 Packtory를 사용하세요. 필요하다면 로컬 SDK 작성을 추가하고 연동 등록·검증은 별도로 진행하세요. 호스팅 공유는 계획 중이며 로컬 자산 관리와 구분됩니다.

거버넌스 및 신뢰

신원·권한·실행 맥락·프로세스 신원·통신 경계·증거 저장소는 제한된 작업을 지원합니다. 그림에 있다는 사실이 검증 증거는 아닙니다.

실행 코어

가장 깊은 계층은 보호된 실행 결정·상태 처리·신뢰 경계·증거 바인딩을 나타냅니다. 공개 라벨은 내부 구현 식별자를 드러내지 않고 역할을 설명합니다. 결정론적 통제 결정이 AI 생성 콘텐츠의 결정성을 의미하지는 않습니다.

평가 질문

오른쪽 패널은 검토자에게 산출물 신원·배포 준비 상태·지원 인터페이스·보안 경계·복구 절차·추적 가능성을 확인하도록 요청합니다. 완료된 검토 상태가 아니라 질문입니다.

참고 자료 및 한계

아키텍처·평가 기준·설치 안내·책임 설명·지원 조건 초안을 함께 사용하십시오. 그림은 Marketplace 제공 여부·상용 출시·인증·운영 성과의 증거가 아닙니다.

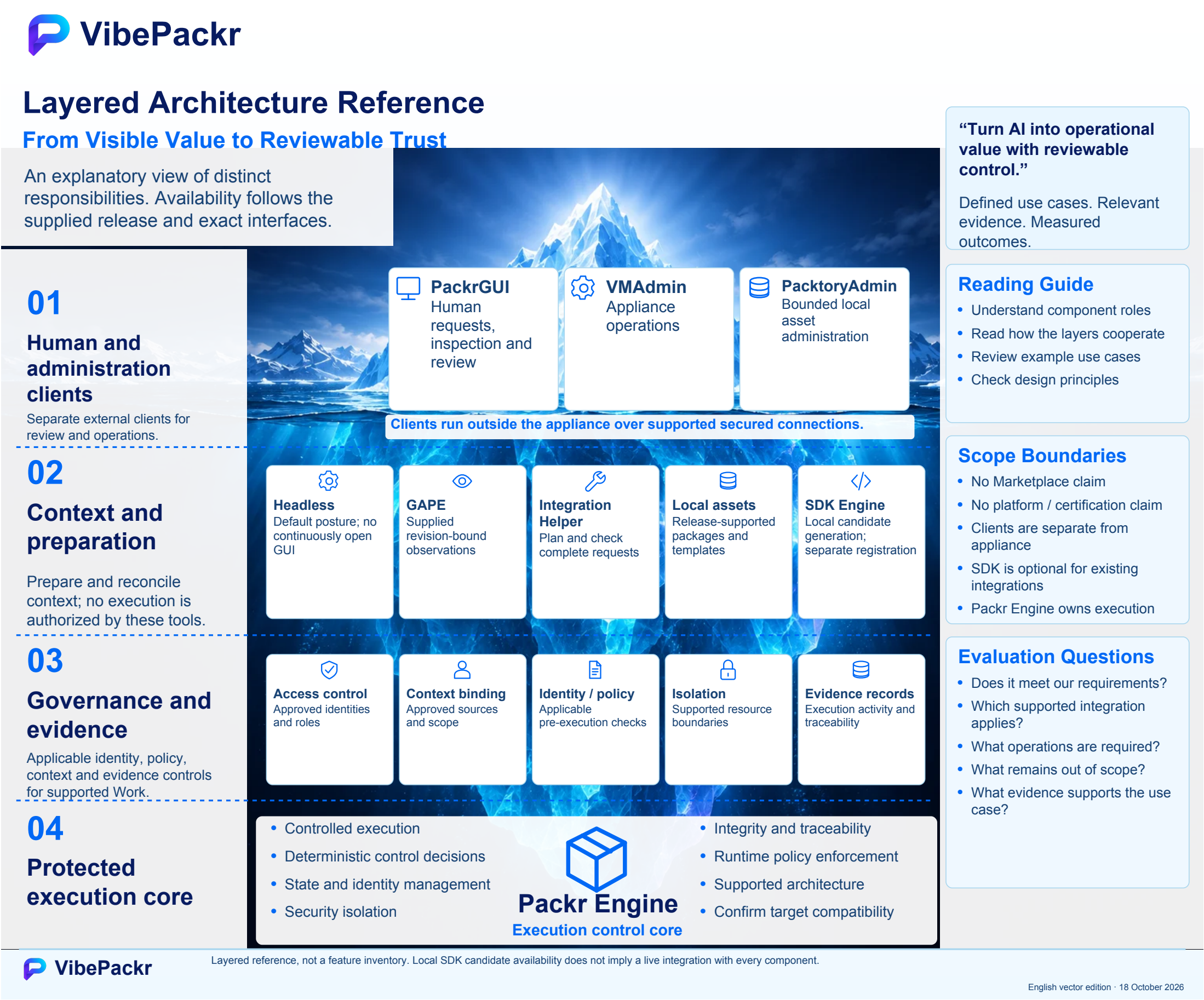
범위 및 한계

개념적 아키텍처 참고 자료이며 제품 화면 캡처나 출시 목록이 아닙니다. 백서는 제한된 로컬 Packtory와 미래의 호스팅·공유 개념을 구분하며, 원격 Rescue 전송은 비활성 상태입니다. SDK는 현재의 필수 구성요소가 아닙니다.

웹사이트에서 이어서 보기

</resources/iceberg-architecture/>

그림 15 · 계층별 아키텍처 참고도



19 공유 자원과 충돌하는 요청

여러 자율 에이전트가 병렬로 동작할 때 조정되지 않은 접근은 데이터 손상·경쟁 상태·교착을 일으킬 수 있습니다. 이 그림은 지원 경로로 전달된 요청의 자원 중복과 순서를 다룹니다. 구체적인 동시 실행·대기열·격리 동작은 선택한 작업 흐름에서 확인해야 합니다.

백서 그림 18 · 영문 전체 참고 그림. 위험 평가 질문이며 검증된 스케줄러나 충돌 방지 보장이 아닙니다.

작업 전에 공유 대상 정의

각각 유용한 두 요청도 같은 자원에 영향을 주거나 변하는 상태에 의존하면 충돌할 수 있습니다. 정확한 대상·허용 변경·관련 정책·권한·현재 전제조건을 식별합니다. 에이전트 추천은 경쟁하는 소유권 문제를 해결하거나 거절된 작업의 우회를 정당화하지 않습니다.

평가 보조 자료로 위험 행렬 사용

다이어그램은 프롬프트 조작·도구 오용·의도하지 않은 변경·데이터 노출·공유 자원에 관한 질문을 실행 통제·증거에 대응시킵니다. 표시는 평가 관계이며 측정된 공격 방어율이나 예방 보장이 아닙니다. 지원 경로를 확인하고 각 관찰 결과를 보존합니다.

웹사이트에서 이어서 보기

[/howto/](#)

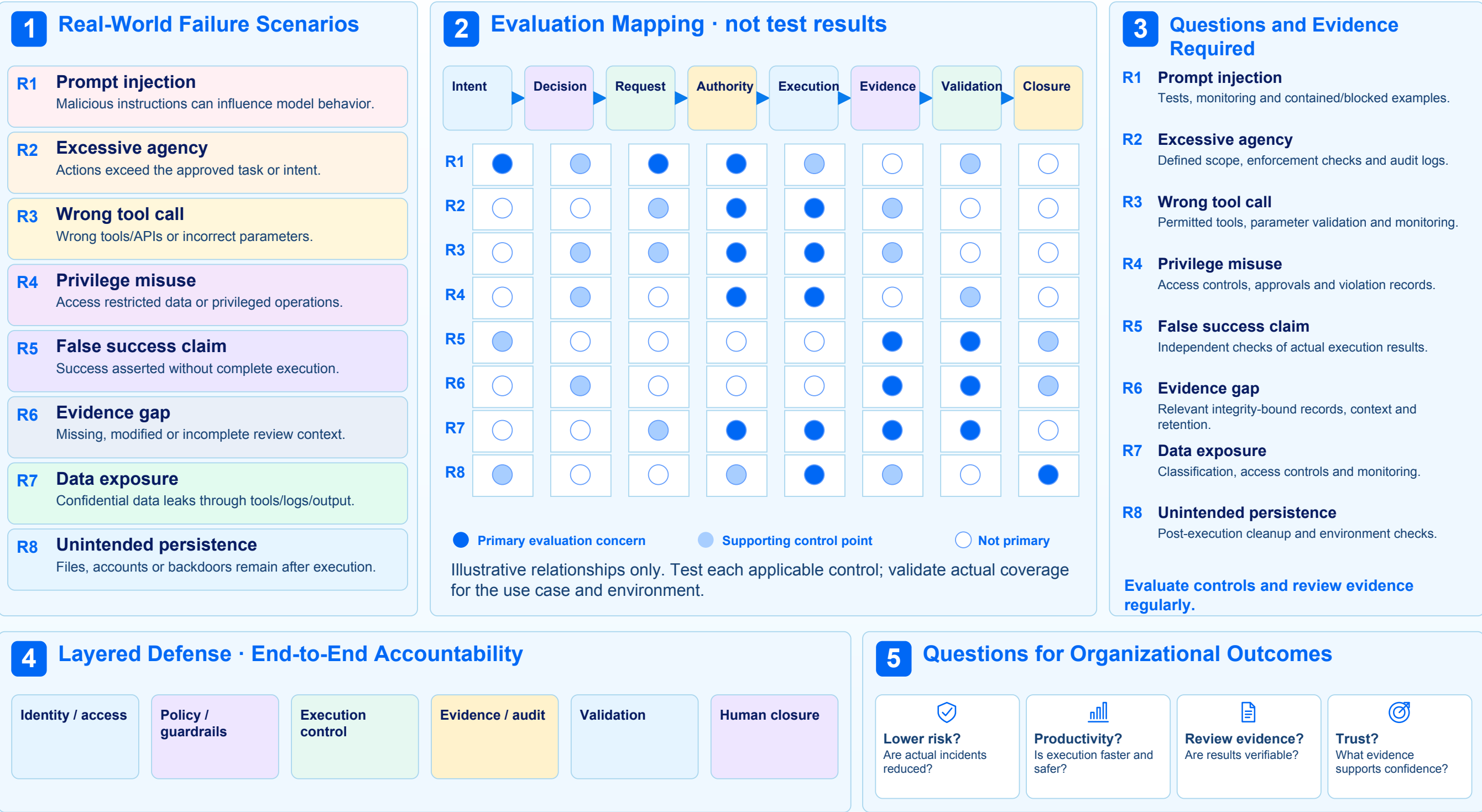
[/resources/enterprise-ecosystem/](#)

그림 18 · AI 위험에서 실행 통제로



From AI Risk to Execution Control

Real scenarios. Evaluation mapping, not test results. Residual risk and bypass paths may remain.



20 AI가 할 수 있는 일과 실행이 허용된 일은 다릅니다.

1. 기반 모델

모델 능력을 제공하며 Work별 권한을 주지는 않습니다. 유능한 모델이 제안 작업의 허가를 독립적으로 부여하지 않습니다.

설명용 예: OpenAI; Anthropic; Google Gemini; Meta Llama; Mistral AI.

2. AI 및 클라우드 플랫폼

모델·도구·관리형 서비스·인프라를 제공합니다. 플랫폼 접근과 Work 허용은 서로 다른 질문에 답합니다.

설명용 예: Google Cloud Vertex AI; Microsoft Azure AI Foundry; AWS Amazon Bedrock; Databricks; NVIDIA.

3. 에이전트 구축 및 오케스트레이션

에이전트를 만들고 흐름을 조정합니다. 단계를 조정한다고 해당 단계가 만들 수 있는 모든 영향을 허가하는 것은 아닙니다.

설명용 예: Microsoft Copilot Studio; LangGraph; crewAI; AutoGen; UiPath; ServiceNow.

4. 데이터 및 지식

승인된 기업 데이터·도메인 맥락을 제공합니다. 접근·처리 권리·출처 정확성·출처 이력에는 각각 담당자가 필요합니다.

설명용 예: Palantir; Databricks; Snowflake; Collibra; Google Cloud BigQuery; Microsoft Fabric.

5. AI 거버넌스

선택한 제품 범위의 AI를 관찰·평가·제한합니다. 거버넌스·보안 통제는 겹칠 수 있으며 이 지도는 공급업체 능력 순위가 아닙니다.

설명용 예: Microsoft Purview; IBM watsonx.governance; Collibra; SAS; Credo AI; Aporia.

6. VibePackr 제품

보호된 Packr Engine이 지원 Work의 권한·정책·범위를 평가합니다. 허용 Work는 지원 제약 안에서 실행될 수 있고 거부 시 해당 요청은 중단됩니다. 결과 검증·연결 증거가 검토를 돕습니다.

7. 보안 및 런타임 보호

운영 환경의 보안·런타임 통제를 구성하고 검증하세요. 이 아키텍처의 공급업체 로고는 예시이므로 실제로 배포할 통제를 선택해 검증해야 합니다.

설명용 예: Palo Alto Networks; CrowdStrike; SentinelOne; Wiz; Snyk; Aqua.

8. ID 및 접근

기존 IAM·PAM·비밀 관리 책임을 유지합니다. 인증·리소스 접근 가능성은 Work별 충분한 권한이 아닙니다.

설명용 예: Microsoft Entra ID; Okta; HashiCorp Vault; CyberArk; BeyondTrust; Ping Identity.

SI가 할 수 있는 일과 실행이 허용된 일은 다릅니다. (계속)

9. 기업 영향 대상

앱·데이터베이스·파일·클라우드 리소스·산업 시스템·API는 설명용 대상 분류이며 시험한 커넥터 목록이 아닙니다. 사용 전 구체적 작업·지원 인터페이스·권한을 확인합니다.

10. 증거·감사·보증

기록은 기술·보안·업무 검토를 지원합니다. 무결성·검증·사람 인수·종결을 구분합니다. 가져온 로그가 과거 작업에 소급 권한을 주지 않습니다.

설명용 예: ELK; Splunk; Microsoft Defender; Chronicle; IBM QRadar; SIEM·GRC 분류.

범위 및 한계

VibePackr로 전달되는 지원 Work의 개념 지도이며 모든 기업 동작을 다루지 않습니다. 공급업체 예는 연동·파트너십·보증·인증을 입증하지 않습니다. ID·보안·거버넌스 책임은 영역 간 겹칠 수 있습니다. 산업 예는 설명용이며 시험된 흐름·산업 승인이 아닙니다. 결과 검증은 필수이며 무결성에 연결된 증거만으로 완전성·진실·사람 인수가 입증되지는 않습니다.

공급업체 이름과 로고는 설명용 예시이며, 확인된 연동·제휴·보증·인증을 의미하지 않습니다. 분류는 겹칠 수 있습니다. 제공 여부와 지원 인터페이스는 확인이 필요합니다.

이 참고 자료는 제품 릴리스·Marketplace·지원·법률 상태를 바꾸거나 서비스 계약을 개정하지 않습니다.

웹사이트에서 이어서 보기

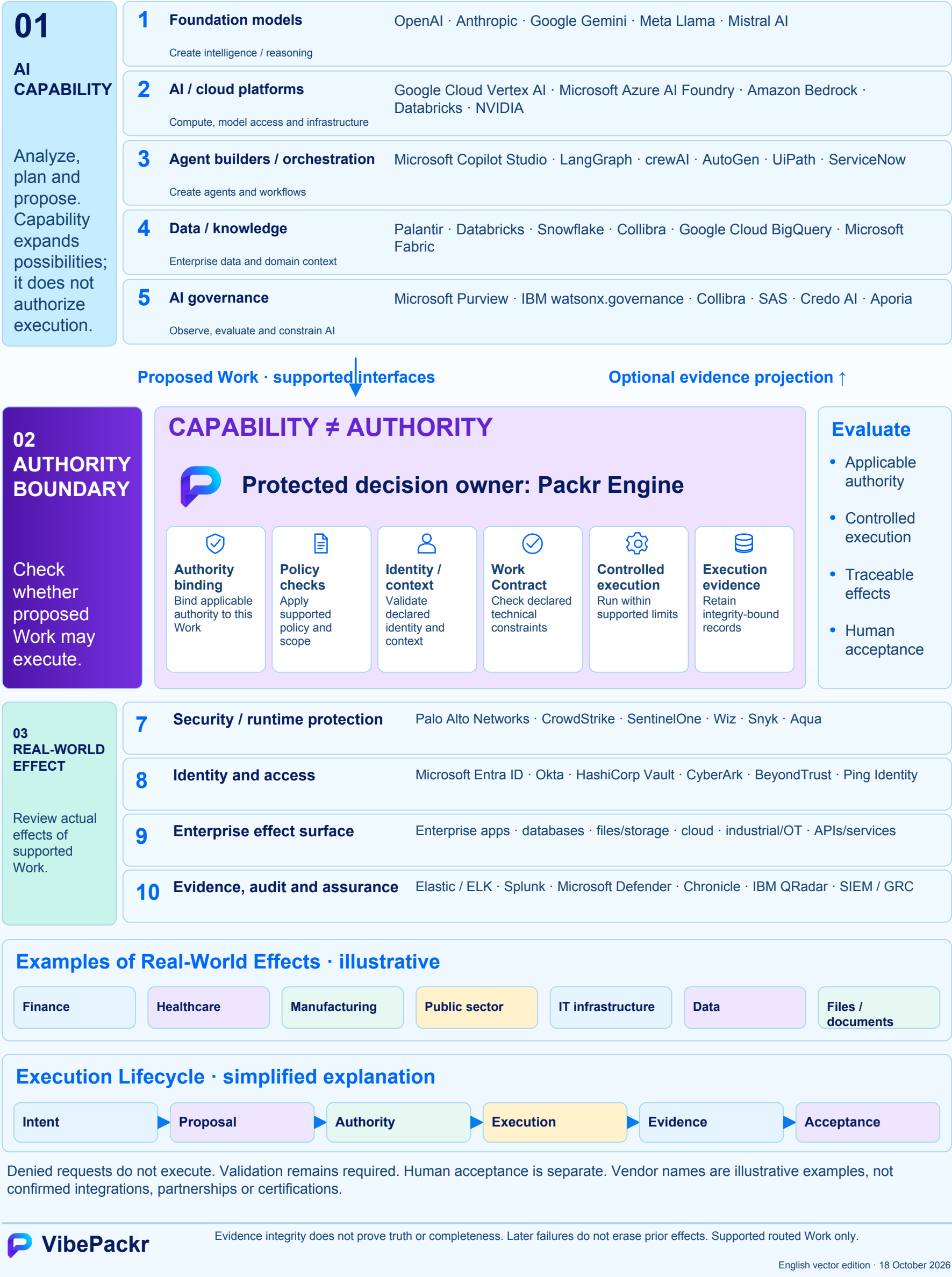
</resources/enterprise-ecosystem/>

그림 25 · 기능과 실행 권한의 구분

 **VibePackr**

What AI Can Do and What It Is Allowed to Execute Are Different.

AI expands possibilities. Supported execution requires governed, Work-specific authority.



21 기업 아키텍처의 통제된 실행

생태계의 역할은 상호 보완적입니다

모델·플랫폼·에이전트·데이터·AI 거버넌스는 서로 다르며 일부 겹칠 수 있는 기능을 제공합니다. 시각적 순서는 필수 진행 순서도, 각 공급업체가 VibePackr와 실제 연결되었다는 증거도 아닙니다.

선언은 지원되는 감사의 입력이 됩니다

정책 소스는 요구사항과 참고 자료를 표현합니다. 그림은 임의의 법률·조직 문서를 강제 가능한 정책으로 자동 해석한다고 주장하지 않습니다. 범위·리비전·허용 형식은 여전히 중요합니다.

하나의 보호된 결정 담당자

Packr Engine이 해당하는 보호된 거버넌스 및 실행 결정을 소유합니다. 중앙 타일은 관련 책임을 설명하며 별도의 권한 엔진을 뜻하지 않습니다. 신원·접근·준비·GUI 동작이 독립적으로 Work 권한을 부여하지는 않습니다.

진입 허용은 성공적인 완료가 아닙니다

허용된 실행에 앞서 적용되는 권한·범위·정책·선행 조건을 평가합니다. 거부된 요청은 실행하지 않습니다. 실행 후에도 관찰된 결과는 검증과 충분한 증거가 필요하며, 사람의 인수는 별개입니다.

거부·실패·불완전은 서로 다릅니다

권한 없음·범위 불일치·정책 거부·신원 불일치·선행 조건 실패는 진입을 막을 수 있습니다. 이후 실행이 실패하거나 증거가 불완전할 수 있습니다. 어느 경우도 부수 효과가 없었거나 롤백이 성공했음을 입증하지는 않습니다.

주변 통제는 고객의 책임으로 남습니다

IAM·PAM·보안 도구·관측 도구는 각각의 소유자와 조건을 유지합니다. 이름과 화살표는 예시이며 확인된 커넥터나 항상 작동하는 보안 보장이 아닙니다. 읽기 전용 투영은 결정 권한을 얻지 않습니다.

준비는 활성화가 아닙니다

업무에 필요한 경우 GAPE로 정해진 맥락을 검토하고 Integration Helper로 후보·계획을 준비하세요. 등록·결합·실행 승인은 별도로 완료해야 합니다. Part.5는 로컬 SDK 작성을 안내하며 전체 Enterprise 통합에는 별도로 지원되는 구현과 검증이 필요합니다.

Non-SI가 통합 노력 없음은 아닙니다

제품화된 지원은 표준 기능과 안내를 제공합니다. 고객별 어댑터·워크플로우 설계·시험·운영에는 고객 또는 구현 담당 소유자가 지정되어야 합니다. 준비가 통합 완료를 약속하지는 않습니다.

증거는 검토를 뒷받침합니다

무결성으로 바인딩된 기록은 산출물 식별과 변경 탐지를 돕습니다. 모든 사건이 관찰되었음을 독립적으로 입증하거나 규제 준수를 인증하거나 사람의 인수·종결 결정을 대체하지 않습니다.

통제 목표에는 평가가 필요합니다

데이터·지식·실행 통제는 선택한 배포 환경에서 평가할 목표입니다. 외부 서비스에는 별도의 처리 경계가 남습니다. 업무 가치·운영 적합성·규정 준수 요건에는 각각의 증거가 필요합니다.

기업 아키텍처의 통제된 실행 (계속)

범위 및 한계

설명을 위한 책임 관계도이며 현재 릴리스 목록·커넥터 목록·인증·자동 통합 파이프라인·성과 보장이 아닙니다. 주 운영 모델과 지원 인터페이스 계약을 우선합니다.

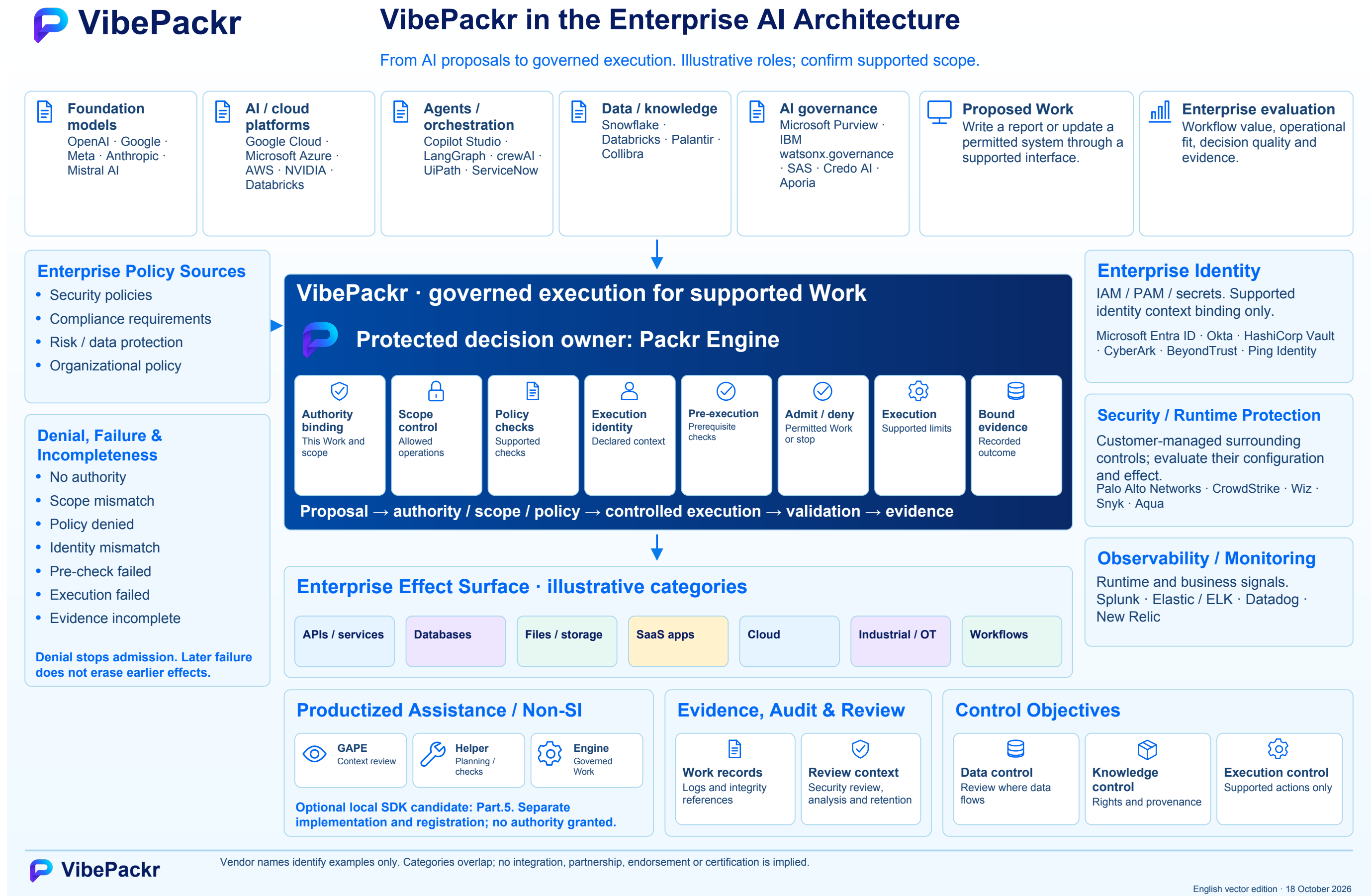
공급업체 이름과 로고는 설명용 예시이며, 확인된 연동·제휴·보증·인증을 의미하지 않습니다. 분류는 겹칠 수 있습니다. 제공 여부와 지원 인터페이스는 확인이 필요합니다.

이 참고 자료는 제품 릴리스·Marketplace·지원·법률 상태를 바꾸거나 서비스 계약을 개정하지 않습니다.

웹사이트에서 이어서 보기

</resources/governed-execution-architecture/>

그림 26 · 기업 AI 아키텍처 안에서의 VibePackr



22 배포 및 신뢰 경계

경계를 올바르게 읽기

경계 운영

목표는 고객이 운영하는 단일 테넌트 어플라이언스입니다. 평가할 지원 플랫폼·테넌트 경계·운영 책임을 확인합니다.

지원 Work 통제

지원 경로로 전달되는 Work의 권한·정책·범위를 확인합니다. 모델 기능과 접근 자격만으로 모든 작업이 승인되지는 않습니다.

외부 처리 명시

외부 AI 서비스를 선택하면 외부 데이터 처리가 발생할 수 있습니다. 사용 전에 데이터 흐름·공급업체 조건·관련 통제를 확인합니다.

운영 모델 비교

책임 유형을 예시합니다. 공급업체의 통제는 선택한 서비스와 배포 방식에 달려 있으며 VibePackr 오픈 목표 모델을 설명하고 일반 제공 상태를 뜻하지 않습니다.

기업 평가를 위한 네 가지 질문

데이터 통제

어떤 데이터가 환경 내부에 남고 어떤 데이터가 선택한 외부 서비스에서 처리됩니까?

실행 주권

이 특정 Work를 누가, 어떤 대상과 범위에 대해 승인할 수 있습니까?

전용 런타임

선택한 어플라이언스 배포에서 실제로 구성되고 검증된 격리 경계는 무엇입니까?

감사 가능성

검토를 뒷받침하는 실행 바인딩 기록은 무엇입니까? 증거 자체가 인증이나 사람의 인수를 입증하지는 않습니다.

릴리스 보증: 평가 체크리스트

아래 단계는 요청할 증거를 식별합니다. 보안 검사 완료를 보고하거나 승인된 릴리스를 발표하지 않습니다.

범위 및 한계

공급업체 통제는 서비스와 배포마다 다릅니다. 제공 여부·지원 범위·릴리스별 검증은 확인이 필요합니다. 이 그림은 제품·지원·Marketplace·법률 상태를 변경하지 않습니다.

고객 운영과 제3자의 책임은 별개로 남습니다. 이 참고 자료는 지원·서비스 계약을 변경하지 않습니다.

웹사이트에서 이어서 보기

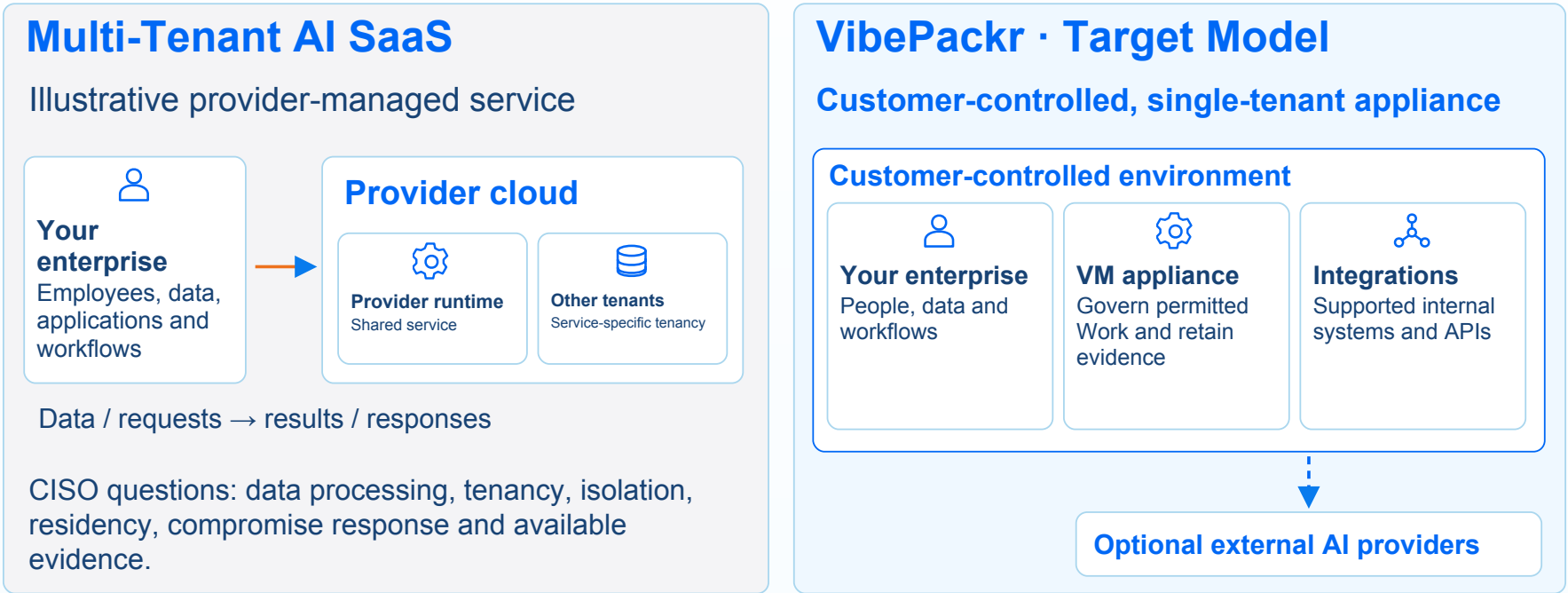
</resources/trust-boundary/>

그림 24 · AI 기능과 배포별 신뢰 경계



AI Capability. Different Trust Boundaries.

Compare who operates the runtime and where execution authority is governed.



23 에이전트 침해만으로 권한이 부여되지는 않습니다.

다섯 단계와 서로 다른 결정.

AI·에이전트 위협

프롬프트 주입·악성 입력·도구 조작·에이전트 조작은 에이전트에 영향을 주려 할 수 있습니다. 위협 예제이며 전체 목록이나 각 공격 방어에 대한 시험 완료 주장이 아닙니다.

기능

추론·계획·파일/네트워크 접근·API/CLI 도구·데이터 처리는 에이전트가 할 수 있는 능력을 설명합니다. 기능은 특정 작업의 허가가 아닙니다.

거버넌스 / 권한

행위 주체·허용 대상·동작·적용 정책 제약·필수 승인을 확인합니다. 에이전트가 스스로 권한을 부여하지 않습니다. 지원 Work의 실행 진입을 허용하기 전에 필수 조건을 충족해야 합니다.

통제된 실행

VibePackr는 지원 경로로 전달된 Work의 권한을 확인하고 정책을 적용하며, 지원 동작의 범위를 제한하고 결과를 기록합니다. 필수 조건을 충족하지 못하면 실행을 거부합니다. 이 경로 밖의 동작에는 해당 플랫폼·운영체제의 통제를 적용하세요.

증거 및 검토

실행 기록·기술적 영수증·산출물·감사 기록을 업무 목적에 맞춰 검토하세요. 권한이 있는 검토자가 결과와 증거를 확인해 업무 인수를 결정하며, 에이전트가 조직을 대신해 인수를 결정할 수는 없습니다.

승인은 조건이며 결론이 아닙니다.

적용 정책이 요구하면 승인을 받습니다. 승인된 실행도 목적·결과 검토가 필요합니다. 기록은 검토를 돕지만 승인·인증·동작의 본질적 안전성 증거는 아닙니다.

고객 운영 어플라이언스. 명시적인 제품·제공자 경계.

이 다이어그램은 Google Cloud를 예로 들어 배포 역할을 설명합니다. 공급업체 이름은 예시이며 제휴 관계를 뜻하지 않습니다. 지원 플랫폼·배포 요건은 해당 릴리스 문서에서 확인하세요.

고객

예시 환경의 프로젝트 IAM·네트워크 구성·배포·운영을 담당합니다. 제품 통제가 고객 운영을 VibePackr로 이전하지 않습니다.

VibePackr 제품

지원 Work의 실행 통제·기록을 제공합니다. 평가할 릴리스·지원 경로·적용 계약을 확인하십시오.

클라우드 인프라

이 예제에서 Google Cloud는 기반 인프라를 제공합니다. 고객 구성·운영 책임은 별개입니다.

AI·에이전트 및 외부 AI

에이전트는 동작을 제안하고 명시적으로 허용된 기능을 사용합니다. 선택한 외부 AI 서비스는 자체 처리 경계를 유지합니다.

에이전트 침해만으로 권한이 부여되지는 않습니다. (계속)

실제로 사용하는 경계 평가.

이 해설은 VibePackr로 전달되는 지원 Work에 적용됩니다. 모든 도구·OS 동작을 가로챌다는 주장이 아니며 모든 공격이 통제된다는 증거도 아닙니다.

지원 연동·필수 권한/승인·고객 운영 통제·선택한 외부 처리·결과 검토 증거를 확인합니다. 적용 계약이 제품 지원·운영 책임을 정의합니다.

이 공개 자료는 보안 검증·인증·새 런타임 기능·서비스 약정을 추가하지 않습니다. 릴리스별 가용성·검증은 확인해야 합니다.

웹사이트에서 이어서 보기

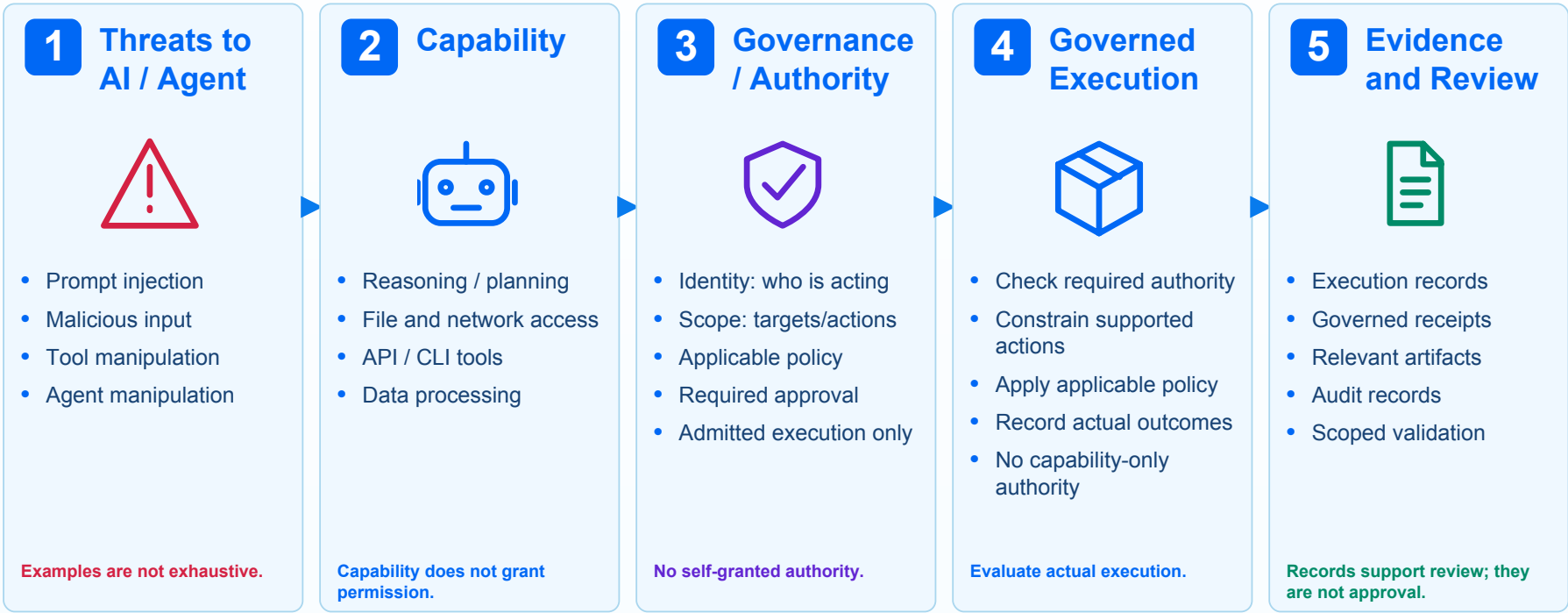
</resources/agent-compromise/>

그림 28 · AI·에이전트 침해와 실행 권한



AI / Agent Compromise and Execution Authority

Compromise alone does not grant authority. Govern supported Work by identity, policy and scope.



Core Security Principles

- ✓ **Capability is not authority. The agent cannot grant itself authority.**
- ✓ **Bind verified identity to permitted scope.**
- ✓ **Evaluate observed results, not self-reports.**
- ✓ **Deny when required conditions are unmet.**
- ✓ **Keep customer and provider boundaries explicit.**

Deployment and Responsibility

- Google Cloud deployment example**
Underlying cloud infrastructure; an example, not endorsement.
- Customer**
Project IAM, network, deployment and operations.
- VibePackr product**
Controls and records for supported Work.
- AI / agent**
Proposes actions; only explicitly permitted capability.
- Customer-operated appliance**
Product controls do not transfer operations to VibePackr.
- External AI services**
Separate processing and trust boundaries.

From Compromise to Governed Decisions

Requests still require applicable authority, policy and scope. Review the purpose and actual results.



Scope of This Diagram

- Supported Work routed through VibePackr only.
- No interception claim for every tool or OS action.
- Not proof that every attack is contained.
- Agreements define support and operations responsibilities.



Reasoning is not authority. Assume compromise, evaluate containment and inspect evidence within the defined boundary.

English vector edition · 18 October 2026

24 하나의 아키텍처. 세 가지 읽는 방법.

역할·참여·통제

독립적인 상자들이 하나의 직교 좌표 공간을 차지합니다. 크기는 정성적인 책임 범위를 설명하며 용량·성능·권한의 양을 측정하지 않습니다.

어떤 종류의 통제인가요?

관찰 전용 → 제한 범위 → 권한 부여 → 바인딩 / 강제 → 정책 내 자율.

인터페이스는 관찰·입력 쪽에 있고 Engine은 강제 영역에 있습니다. 이 투영에서 X4는 의도적으로 비워 두었습니다.

언제 참여하나요?

이해 → 준비 → 승인 → 바인딩 → 실행 → 관찰 → 검증 → 종결 → 복구.

긴 상자는 작업 전반의 더 많은 책임에 걸쳐 있습니다. 이는 참여 지도이며 실제로 저장되는 상태 머신의 정확한 순서가 아닙니다.

어떤 아키텍처 역할인가요?

인터페이스 · 아키텍처 / 통합 · 정책 및 권한 · 런타임 / 실행 · 관찰 · 증거 및 신뢰 · 외부 효과.

상자 색상은 주요 평면을 나타냅니다. 하나의 기능은 동일한 보호된 결정 소유자를 유지하면서 여러 평면에 관여할 수 있습니다.

전체 아키텍처 공간 살펴보기

공통 원점의 축에서 시작하십시오. 번호가 붙은 상자를 찾은 뒤 아래 구성요소 범례를 사용하십시오. 세부 내용을 확대하려면 뷰어를 열고, 인쇄하려면 A4 PDF를 다운로드하십시오.

선을 읽는 방법

각 선분은 하나의 좌표를 바꿉니다. 색은 해당 축을 나타내며 연결의 신뢰·성공·활성 상태를 뜻하지 않습니다.

하나의 연결도 꺾이는 곳에서 색이 바뀔 수 있습니다. 화살촉이나 교차점이 권한을 부여하지 않으며 시각적 교차만으로 공유 인터페이스가 성립하지 않습니다.

경계를 드러나게 유지하기

점선 External Systems 상자는 일반적인 대상 범위를 나타냅니다. 범용 실행 연결은 없습니다. 아래의 OS 및 네트워크 참고 자료는 제품의 Z 평면 밖에 있습니다.

전체 SVG는 JavaScript 없이 직접 열립니다. 브라우저 확대 기능을 사용하거나 PDF를 다운로드하십시오.

15개 역할, 서로 다른 책임

번호는 다이어그램과 일치합니다. Policy Manager와 Authority Controller 같은 이름은 기능적 책임을 나타내며 별도 배포 제품을 의미하지 않습니다.

사용자 인터페이스(Human Interface)

작업 전반에서 의도·검토·인수 입력을 제공합니다. 사람의 결정은 지원되는 검사를 거쳐 입력되며 화면을 사용한다는 사실이 독립적으로 실행을 승인하지는 않습니다.

하나의 아키텍처. 세 가지 읽는 방법. (계속)

에이전트 인터페이스(Agent Interface)

타입이 지정된 요청을 제출하고 결과를 조회합니다. 에이전트가 작업을 제안할 수 있다는 사실이 진입 검사를 우회하거나 실행 권한을 얻는 근거가 되지 않습니다.

개발자 인터페이스(Developer Interface)

준비·바인딩 영역에서 선언과 제한된 통합 입력을 제공합니다. 확장 기능과 실행 허가는 별개입니다.

GAPE

이해 단계에서 탐색과 아키텍처 이해를 지원합니다. 관찰 내용은 준비의 참고가 되며 새로운 제품 권한을 만들지 않습니다.

Integration Helper

제한된 통합 준비를 위해 지원되는 입력을 검사하고 정리합니다. 준비된 후보나 계획이 연결·등록·승인된 런타임 통합을 뜻하지는 않습니다.

SDK Engine

지원 확장에는 공개 타입 인터페이스와 호환성 규칙을 사용하세요. 생성·업무 흐름 연결·전달 요건은 해당 패키지에 제공된 안내를 확인하세요.

정책 관리자(Policy Manager)

실행 전 정책 정의와 제약 입력을 나타냅니다. 적용되는 보호된 결정은 Packr Engine 안에 남습니다.

권한 통제기(Authority Controller)

승인·바인딩 단계의 신원·범위·진입·바인딩 검사를 나타냅니다. 실행 거버넌스와 동일한 보호된 Rust 소유자에 속합니다.

위험 분석기(Risk Analyzer)

통제된 진입에 위험 평가 입력을 제공합니다. 분석은 독립적인 허가의 출처나 무위험 운영 보장이 아닙니다.

Packr Engine(Rust)

보호된 통제 실행 결정·전이·종결 게이트를 소유합니다. 바인딩 → 실행 → 종결에 걸친 범위는 이 뷰의 중심에 강제 기능을 배치합니다.

관찰자(Observer)

실행·관찰 단계에서 타입이 지정된 상태와 작업 관찰 정보를 읽습니다. 읽기 전용 가시성은 강제 권한이 아니며 작업을 승인할 수 없습니다.

검증자(Verifier)

검증·종결 단계의 결과 및 증거 검증을 나타냅니다. 검증 결정은 보호된 소유자에 남으며 검증이 실행 권한을 부여하지는 않습니다.

ETS

증거 및 신뢰 역할은 범위가 정해진 제품 자산 경로의 신원·무결성·계보·보존을 다룹니다. 모든 Work에 ETS 참조가 있거나 증거가 실행이라는 뜻은 아닙니다.

하나의 아키텍처. 세 가지 읽는 방법. (계속)

복구 관리자(Recovery Manager)

종결·복구 단계의 권한이 부여된 백업·복원·상태 대조를 나타냅니다. 현재 작업 권한은 여전히 필요하며 임의의 외부 되돌리기를 주장하지 않습니다.

외부 시스템(External Systems)

고객이 통제하는 대상 경계로서 클라우드·온프레미스 시스템·데이터베이스·기업 애플리케이션·기타 해당 대상을 포함합니다. 분류가 입증된 커넥터 목록이나 모든 산업·장치 지원을 뜻하지는 않습니다.

요청 하나의 준비부터 검토까지

범위가 제한된 읽기 작업 하나를 준비한다고 가정해 보십시오. 아래 순서는 역할을 설명하며 새로 실행한 종단 간 시험·자동 파이프라인·모든 Work의 필수 경로가 아닙니다.

대상 이해 · 04

사용 가능한 GAPE 관찰 자료로 구성요소와 관계를 검토합니다. 의도한 작업의 요구를 확정합니다. 관찰된 구조는 맥락을 제공하며 허가를 주지는 않습니다.

지원되는 입력 준비 · 03, 05, 06

지원 선언으로 기능을 설명하세요. Helper 결과에서 후보·누락 요건·거부 사유를 확인한 뒤 정규화와 연동을 검증하고 사용하세요.

권한 및 바인딩 평가 · 07, 08, 09, 10

지원되는 실행 전에 정확한 신원·범위·적용 제약·선행 조건을 평가해야 합니다. 준비가 작업을 자동 등록·바인딩·승인하지는 않습니다.

기록된 결과 살펴보기 · 10, 11, 12, 13

허용된 작업은 정확한 신원을 따라 상태·결과 검증·사용 가능한 증거를 확인합니다. 실제 로컬 실행은 보존된 Headless 예시를 읽고, 명시된 버전과 범위의 한계를 유지하십시오.

권한 범위 안에서 검토·종결·복구 · 01, 14

해당 보고서를 열고 리비전을 확인하며 검증과 사람의 인수를 구분합니다. 복구는 별도로 통제되는 작업이며 실패만으로 롤백을 입증하거나 이전 효과를 없앨 수 없습니다.

예시들은 별개의 기록입니다. 연결된 Helper·Headless·GUI 예시는 각각 관찰된 결과를 설명합니다. 하나의 연속 실행이나 새로 검증된 고객 배포로 제시하지 않습니다.

XYZ 공간 밖의 두 참고 자료

운영체제 상호작용과 네트워크 통신은 관련되지만 서로 다릅니다. 파일 쓰거나 로컬 IPC 교환이 반드시 네트워크 스택을 통과하지는 않습니다.

OS 채널 구조(OS Channel Fabric)

여섯 채널 계열은 프로세스·런타임, IPC, 파일시스템·저장소, 네트워크, 장치·플랫폼, OS·커널 서비스를 정리합니다.

선택된 선은 통제된 프로세스 시작·타입 지정 로컬 IPC·영속 상태 저장을 나타냅니다. Observer의 선택된 IPC 관계는 읽기 전용입니다. 연결되지 않은 채널 분류는 참고 맥락이며 직접 접근을 주장하지 않습니다.

하나의 아키텍처. 세 가지 읽는 방법. (계속)

네트워크 / OSI 통신 참고 자료

7계층 참고 자료는 애플리케이션 프로토콜부터 물리·가상 네트워크 링크까지의 통신 개념을 설명합니다.

네트워크 채널 계열만 이 참고 자료에 연결됩니다. QUIC 같은 최신 프로토콜은 전통적인 경계를 넘으며, 라벨이 배타적인 매핑이나 나열된 모든 프로토콜의 제품 지원을 주장하지는 않습니다.

한계를 명시한 구조 설명

다이어그램은 구현·계약 증거와 대조되었습니다. 책임 투영이며 배포 목록·새 런타임 시험·지원 커넥터 목록·릴리스 승인이 아닙니다.

통제권은 사람에게 남습니다. 구성은 위임할 수 있습니다. 거버넌스는 위임하지 않습니다.

이 투영은 인증·성능 결과·고객 배포·새 공급업체 실행을 주장하지 않습니다. 여기서 X4가 비어 있다는 도식상의 선택은 기능이 없다는 판정이 아닙니다. 지원 범위와 제공 여부는 선택한 릴리스 및 배포에 따라 달라집니다.

기업 AI를 위한 통제된 실행 제어 평면

같은 AI, 다양한 인터페이스, 더 안전한 내일.

웹사이트에서 이어서 보기

</resources/xyz-architecture-space/>

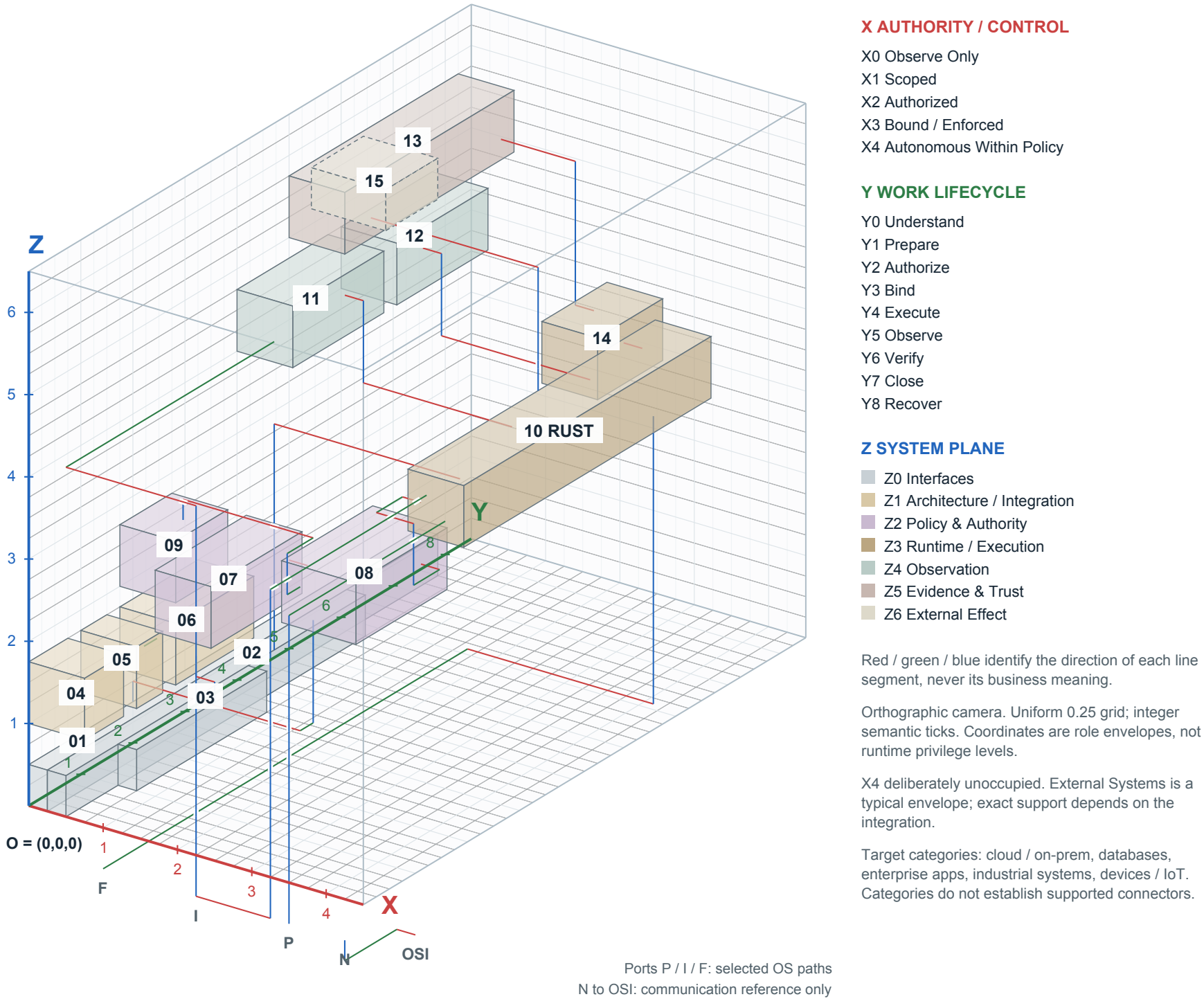
그림 27 · XYZ 아키텍처 공간

VibePackr

XYZ Architecture Space

Position = architectural role Volume = responsibility coverage Connections = governed interaction

ENGINEERING PROJECTION / R0 / 05 OCT 2026



COMPONENT KEY

- 01 Human Interface
- 02 Agent Interface
- 03 Developer Interface
- 04 GAPE
- 05 Integration Helper

- 06 SDK Engine
- 07 Policy Manager*
- 08 Authority Controller*
- 09 Risk Analyzer*
- 10 Packr Engine (Rust)

- 11 Observer
- 12 Verifier*
- 13 ETS*
- 14 Recovery Manager*
- 15 External Systems

* Functional projections share the protected Rust owner; they do not imply separate deployed services. GAPE grants no new authority. SDK API surface exists; generated/workflow SDK scope is not proven.

OS CHANNEL FABRIC

System interaction channels | reference families

P PROCESS & RUNTIME

process / thread / signal
credentials / namespace / cgroup
runtime state

F FILESYSTEM & STORAGE

file / directory / file descriptor
mount / volume / durable state
temporary / cache state

D DEVICE & PLATFORM

device / driver / GPU / accelerator
VM / hypervisor / hardware
platform API

I IPC & COMMUNICATION

stdin / stdout / stderr / pipe
Unix Domain Socket / named pipe
shared memory

N NETWORK & CONNECTIVITY

socket / TCP / UDP / QUIC
interface / route / loopback / VPN
proxy / firewall

K OS / KERNEL SERVICES

syscall / scheduler / resource control
security / identity / audit / trace

NETWORK / OSI SUBSTRATE

Communication reference model

L7 Application

HTTP / gRPC / API / app protocols

L6 Presentation

encoding / serialization / encryption representation

L5 Session

session / connection state (where applicable)

L4 Transport

TCP / UDP / QUIC (cross-layer behavior)

L3 Network

IP / routing

L2 Data Link

Ethernet / Wi-Fi / VLAN / switching

L1 Physical

physical / virtual network link

Only network channels map to OSI. Protocol mappings are approximate, not exclusive. Catalogs do not certify product support.

Capability ≠ Authority • Observation ≠ Enforcement • Verification ≠ Authority
Evidence ≠ Execution • Recoverability ≠ Authority • Human remains in control.

Configuration may be delegated. Governance is not.

VibePackr | Governed Execution Control Plane for Enterprise AI

Position defines role. Volume defines responsibility. Connections define governed interaction.

Same AI. Different Interfaces.

A Safer Tomorrow.

25 로컬 기록 사례: 하나의 식별자를 따라가기

Headless R234: 기록된 로컬 Work 1건

2026년 10월 4일 사례는 준비·거절된 입력·수정된 의도·실행·보고서 검증을 따라갑니다. 기록에는 실행 횟수 1, 검증 PASSED, 사람의 인수 필요·미기록이 있습니다. 상태 RUNNING과 상태 확인·준비도 UNKNOWN은 서로 다른 관찰이며, 이 실습을 다른 환경의 전제조건을 무시할 허가로 사용하지 않습니다.

거절된 준비도 세션 메타데이터를 저장했습니다. 첫 결과를 보존합니다. 수정 후에는 다른 화면을 얻으려고 다시 제출하지 말고 반환된 Work를 확인합니다. PDF·JSON 파일 해시와 정본 보고서 다이제스트는 서로 다른 식별 질문에 답합니다.

PackrGUI R11: 정확한 보고서 탐색·확인

GUI 사례는 다른 Work입니다. 로컬 R11 후보가 보존 보고서 리비전 16을 찾아 표시하고, 해당 PDF를 Preview에서 연 뒤 Work로 돌아왔습니다. 보고서는 자동화 완료·사람의 인수 대기를 기록합니다. Open JSON은 실행하지 않았습니다. 보고서를 열거나 인쇄해도 Work를 인수한 것은 아닙니다.

기록 읽기 실습으로 사용

연결된 설명은 날짜·버전·실패·남은 판단을 보존합니다. 실제 터미널·새 실행·고객 배포·운영 인수가 아니라 기록된 로컬 사례입니다. 별도의 승인된 평가를 정의할 때 PoC 공통 가이드를 사용합니다.

웹사이트에서 이어서 보기

</docs/headless-worked-run-en.html>

</docs/packrgui-final-report-en.html>

</guides/poc/>

26 필요한 매뉴얼 선택: Part.1~8

Part.1 · 설치·초기 연결

OS·패키지·초기 연결 전제조건을 선택합니다.

Part.2 · GAPE 관찰·비교·공유

범위가 정해진 리비전을 관찰하고 반환 아키텍처를 확인합니다.

Part.3 · Integration Helper 사용

선언 전에 준비하고 선언 후 검증·인계를 진행합니다.

Part.4 · Contract·Document 작성

의도·제약·입력·검토 맥락을 선언합니다.

Part.5 · SDK Engine 실습·연동 후보

맞춤 작성이 필요할 때 로컬 어댑터 후보를 생성합니다.

Part.6 · Builder·추가 Pack 사용

기존 승인 Pack으로 충족되지 않는 경우 후보를 준비합니다.

Part.7 · PackrGUI·헤드리스 사용

Work 식별자·실행·검증·보고서 검토를 따라갑니다.

Part.8 · 운영·문제 해결·지원

실패 시도를 보존하고 문제를 분류한 뒤 최소 지원 기록을 준비합니다.

웹사이트에서 이어서 보기

[/docs/](#)

[/docs/manuals/index.html](#)

[/docs/manuals/Part_01_Installation.html](#)

[/docs/manuals/Part_02_GAPE.html](#)

[/docs/manuals/Part_03_Integration_Helper.html](#)

[/docs/manuals/Part_04_Document.html](#)

[/docs/manuals/Part_05_SDK_Engine.html](#)

[/docs/manuals/Part_06_Builder.html](#)

[/docs/manuals/Part_07_PackrGUI.html](#)

[/docs/manuals/Part_08_Operations.html](#)

27 네 가지 실무 가이드와 문제 해결 인계

PoC 공통 가이드

평가 질문·버전·담당자·전제조건·허용 작업·마무리 증거를 정의할 때 시작합니다. 기존 기록 읽기, 승인된 로컬 실습 재현, 고객 평가 계획을 구분합니다.

Google 심사자 가이드

공급업체가 작성한 검토 경로와 인용 요구사항으로 제공 증거와 추가 검사를 구분합니다. 검토 지원 자료이며 Google이 작성하거나 승인한 안내가 아닙니다. Amazon·Microsoft 심사자 가이드는 준비 중입니다.

온프레미스 가이드

환경에 맞게 Online·Offline을 선택하고 패키지 무결성, OS·아키텍처·네이티브 전제조건을 확인합니다. 포함된 Rust 의존성 트리는 문서의 빌드 경로를 지원하며 OS SDK·링커·고객 권한이나 다른 도구의 모든 전제조건을 대신하지 않습니다.

Custom Execution 가이드

작업별 준비·입출력 예시·검증 절차를 사용합니다. Guide Pack은 문서 묶음이며 다운로드가 실행 Pack을 등록하거나 Work Authority를 부여하지 않습니다.

단계가 실패했을 때

정확한 요청·반환 사유·종료 코드·결과 디렉터리를 보존합니다. 변경 전에 명시된 전제조건이나 타입을 확인합니다. 다음 담당자에게 도구·버전·기대 결과·실제 결과·허용 데이터 범위·공유 가능한 관련 산출물 참조를 전달합니다. 인증 정보·원본 기밀 로그·비공개 업무 기록을 보내지 않습니다.

웹사이트에서 이어서 보기

</guides/>

</guides/poc/>

</guides/google-reviewer/>

</guides/on-premises/>

</guides/custom-execution/>

[/docs/manuals/Part_08_Operations.html](/docs/manuals/Part_08_Operations.html)

28 이 판에서 사용하는 용어

Work

범위와 식별자를 갖춘 통제 대상 업무 단위입니다.

Work Authority

해당 정책과 범위 아래 특정 작업에 부여되는 실행 권한입니다.

Contract·Document

기술 선언과 검토된 지원 자료이며, 준비와 실행 허가는 별도입니다.

PINM

업무 지식 자산화 모델의 내부 인텔리전스 코어입니다.

Custom Pack

사용자가 정의하고 식별·검토한 재사용 지식·기능 자산입니다.

Packtory

지원되는 로컬 수명주기에서 검색·리비전·저장·재사용을 통제합니다.

기술 리시트

기술적 처리 결과를 담은 기록이며 업무 인수와 구분됩니다.

검증·인수

검증은 명시된 기준을 확인하며 최종 인수는 책임 조직이 판단합니다.

웹사이트에서 이어서 보기

</architecture/>

</docs/manuals/index.html>

29 출처·읽기 경로·판 안내

2026년 10월 18일, 대한민국 서울 VibePackr Co., Ltd. 발행. 영문판과 한국어판은 하나의 장·그림 목록을 공유합니다. 본문·캡션·탐색은 각 언어로 제공하며, 두 판 모두 아키텍처 SVG 표기는 영어로 유지합니다.

현재 웹사이트와 매뉴얼

이 판은 현재 웹사이트 소개·아키텍처·참고 설명, Part.1~8, 네 가지 실무 가이드와 정합하게 작성했습니다. 연결된 페이지에서 상세 전제조건·전체 요청 파일·명령·문제 해결 사례를 제공합니다. 설치·운영은 해당 전체 절차를 따르며 이 기술 백서는 구조와 다음 읽기 경로를 설명합니다.

그림 식별자와 현재 판

그림 번호는 웹사이트에서 사용하는 참조 식별자를 유지하며, 그림 목차에 이 판의 수록 대상을 표시합니다. 그림 29~32는 Non-SI 모델·복잡성·Pack 시스템·실제 도구 흐름을 연결합니다. 이 영문·한국어 두 판이 현재 다운로드 가능한 기술 백서입니다.

기술 설명과 운영 범위 구분

릴리스 문서에서 제공 버전·지원 인터페이스·대상 환경 조건을 확인합니다. 이 백서는 법률 조건·인증·Marketplace 승인·서비스 약속을 추가하지 않습니다. 기존 기록 사례는 자체 버전과 관찰 범위를 유지합니다. 고객 배포·실행·최종 인수에는 각각 해당 권한이 필요합니다.

웹사이트에서 이어서 보기

/

[/architecture/](#)

[/resources/](#)

[/docs/](#)

[/guides/](#)

[/legal/](#)