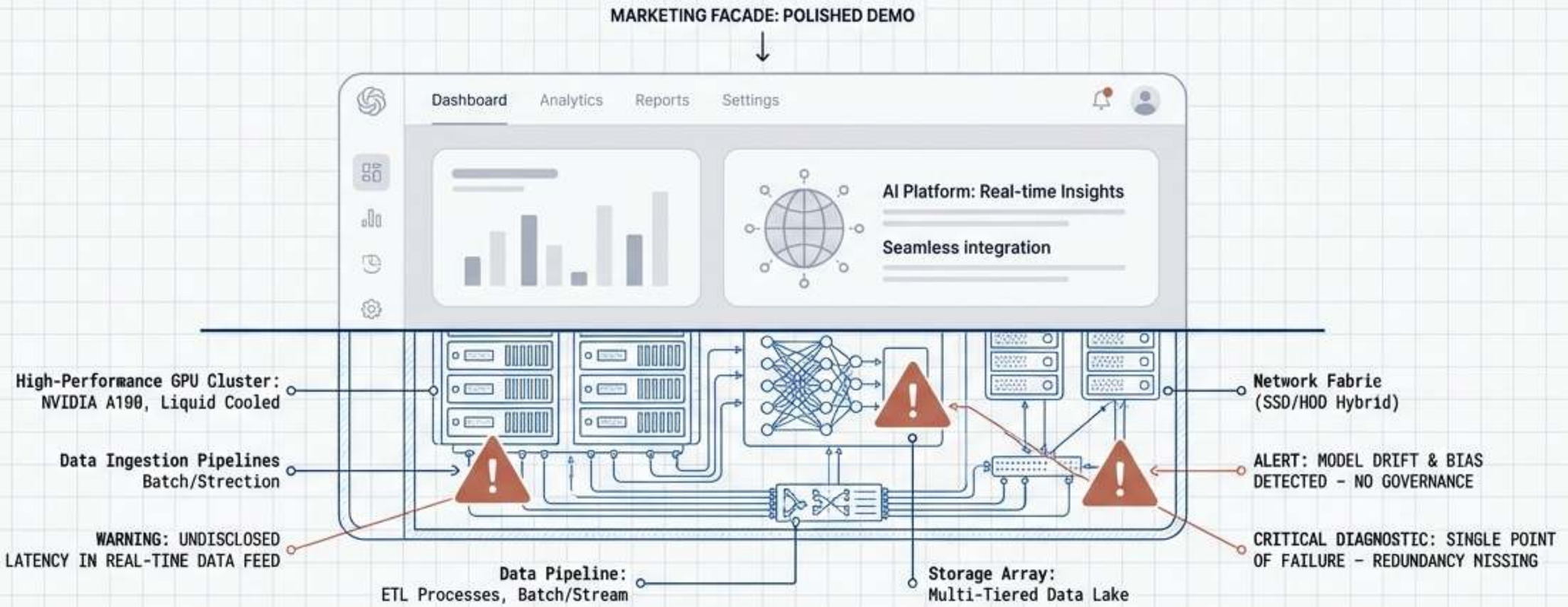
X-Raying AI Vendors

A diagnostic framework for legal and IT procurement to separate marketing promises from structural reality



PROCUREMENT ASSESSMENT

Criteria	Status
Vendor Claims	[✓] Verified
Contractual Obligation	[×] Discrepancy
Technical Audit	[!] Risk Identified

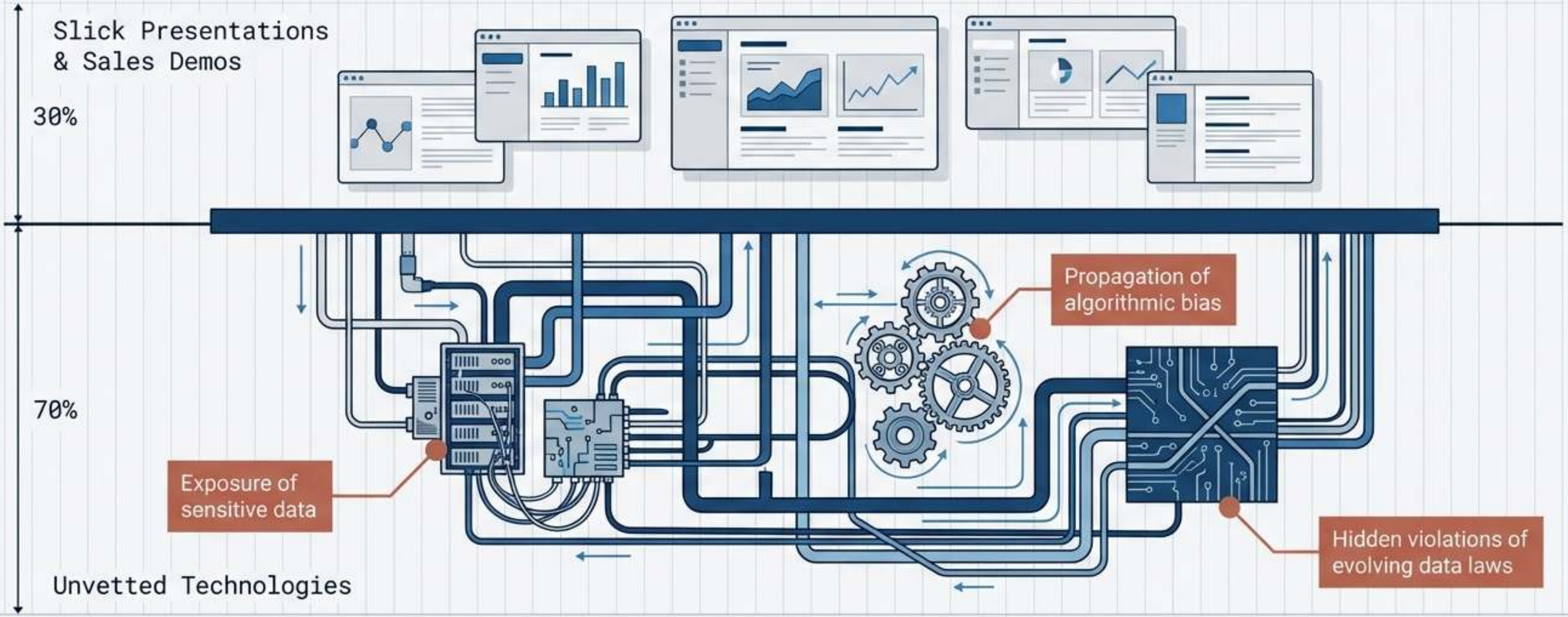
TECHNICAL DIAGNOSTIC SUMMARY

Component	Marketing	Reality	Risk Level
Latency	Sub-millisecond	>S0Oms Average	High [Terracotta Alert]
Scalability	Infinite	Limited by Hardware	Medium [Terracotta Alert]
Security	Enterprise Grade	Basic Encryption	High [Terracotta Alert]

NotebookLM

The pressure to adopt AI obscures the hidden structural risks

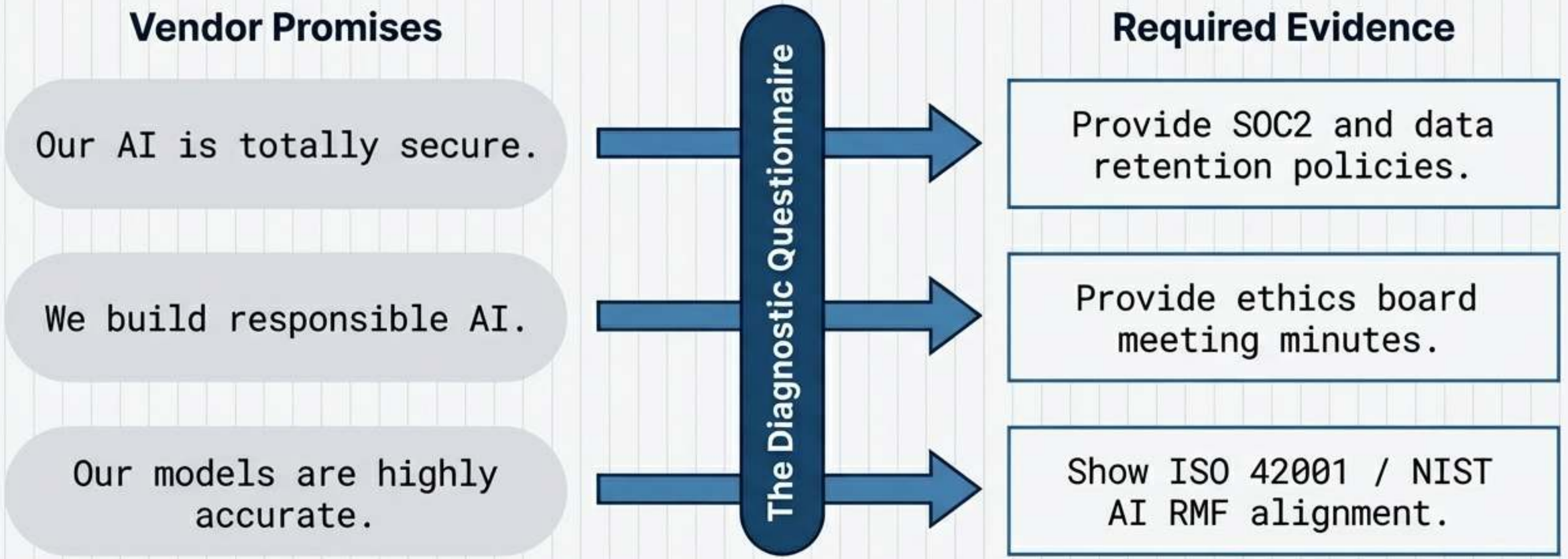
Vendors know leaders are under real pressure to adopt AI tools quickly.
Every vendor claims their product is secure, fair, and compliant.



NotebookLM

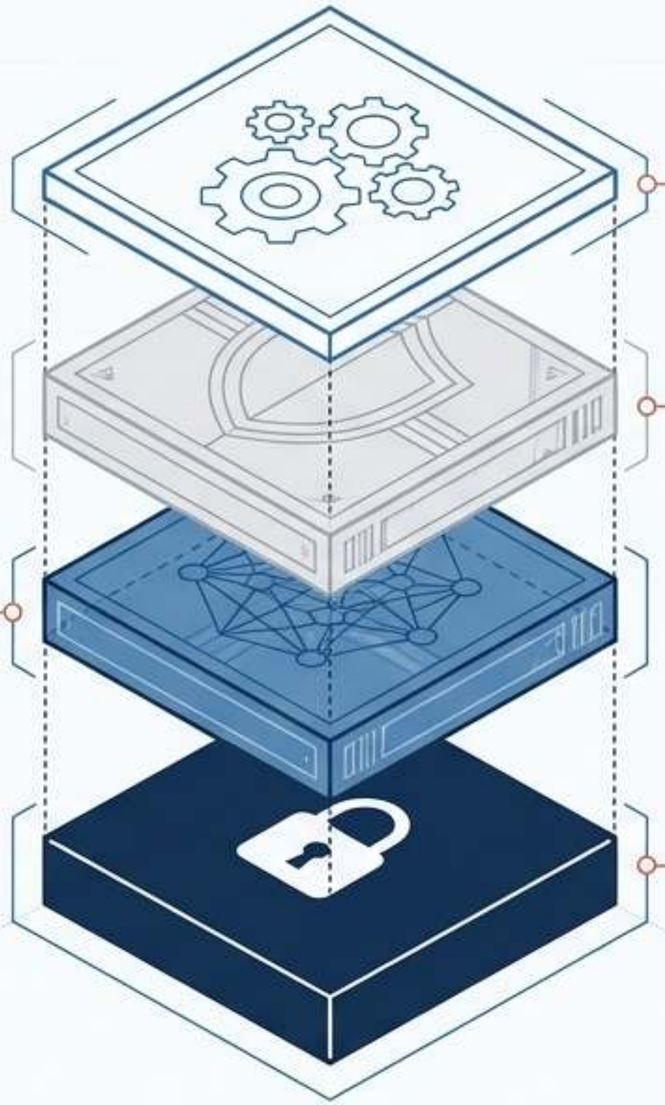
Demand documentation, not promises

Slick presentations rarely reveal a vendor's actual security posture or compliance readiness.



NotebookLM

The four pillars of vendor due diligence



04. Support, Implementation & Scalability

03. Compliance, Governance & Ethics

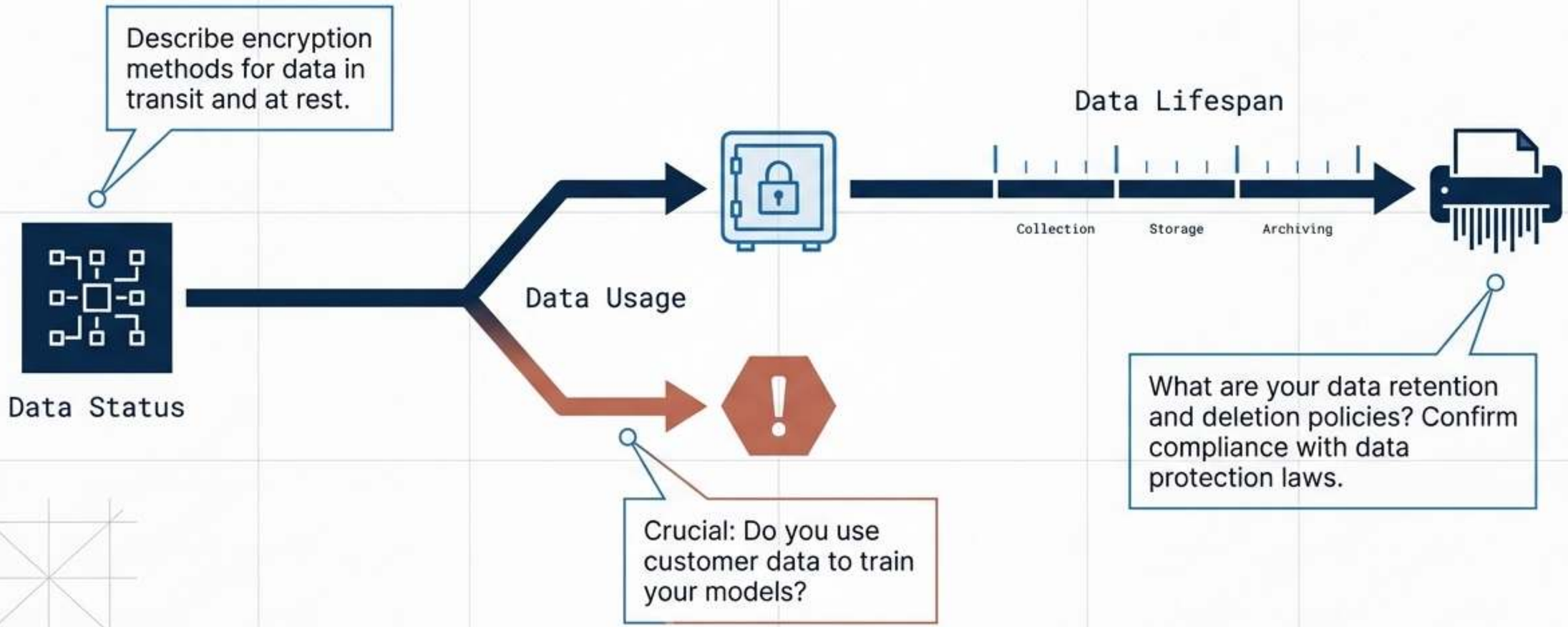
02. Model Performance & Explainability

01. Data Privacy & Security

NotebookLM

Pillar 1 requires mapping the exact lifecycle of your data

If the vendor can’t answer these questions with specifics, that tells you something important.

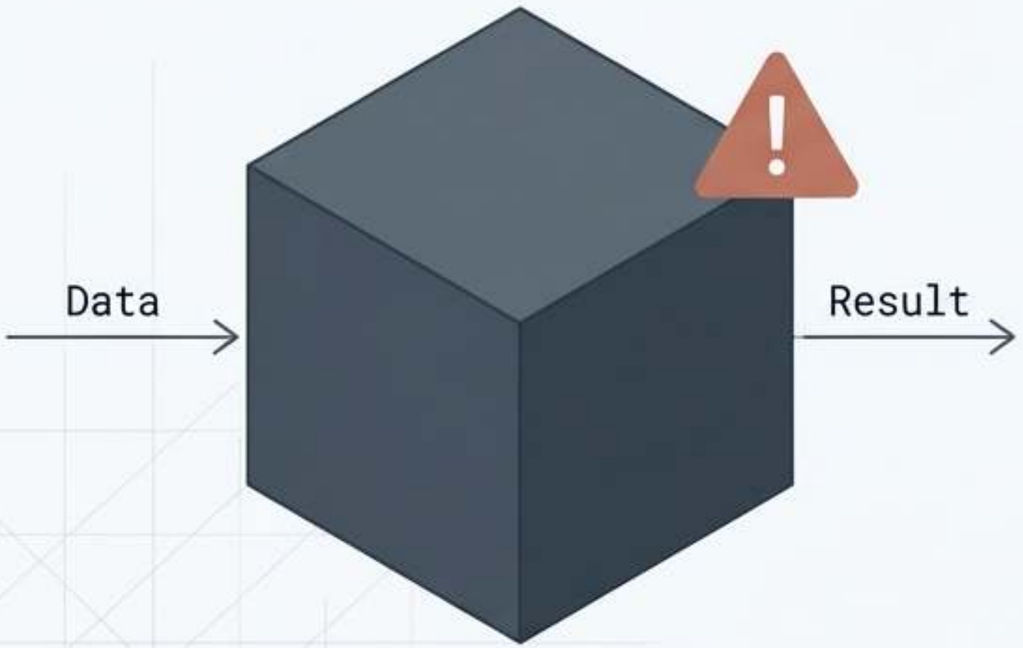


NotebookLM

Pillar 2 demands turning the algorithm from a black box to a glass box

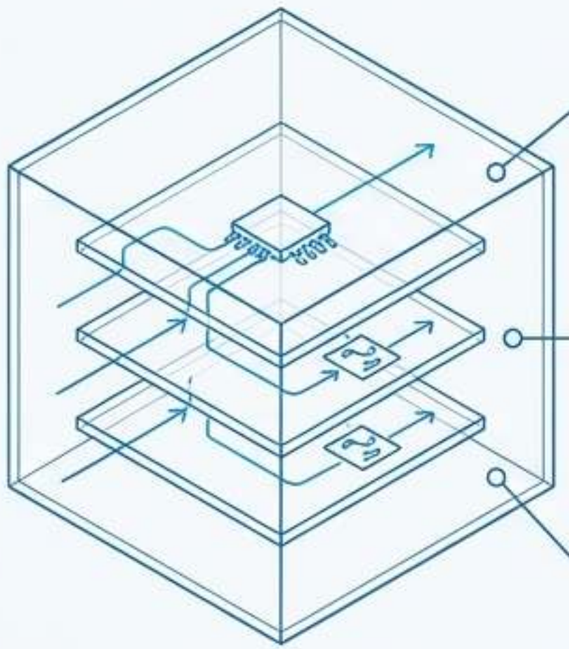
A vendor who has done this work will have materials ready. One who hasn't will struggle to answer.

The Black Box



Unvetted AI

The Glass Box



Documentation: Model training, validation, and testing records.

Frameworks: Alignment with ISO 42001 or NIST AI RMF.

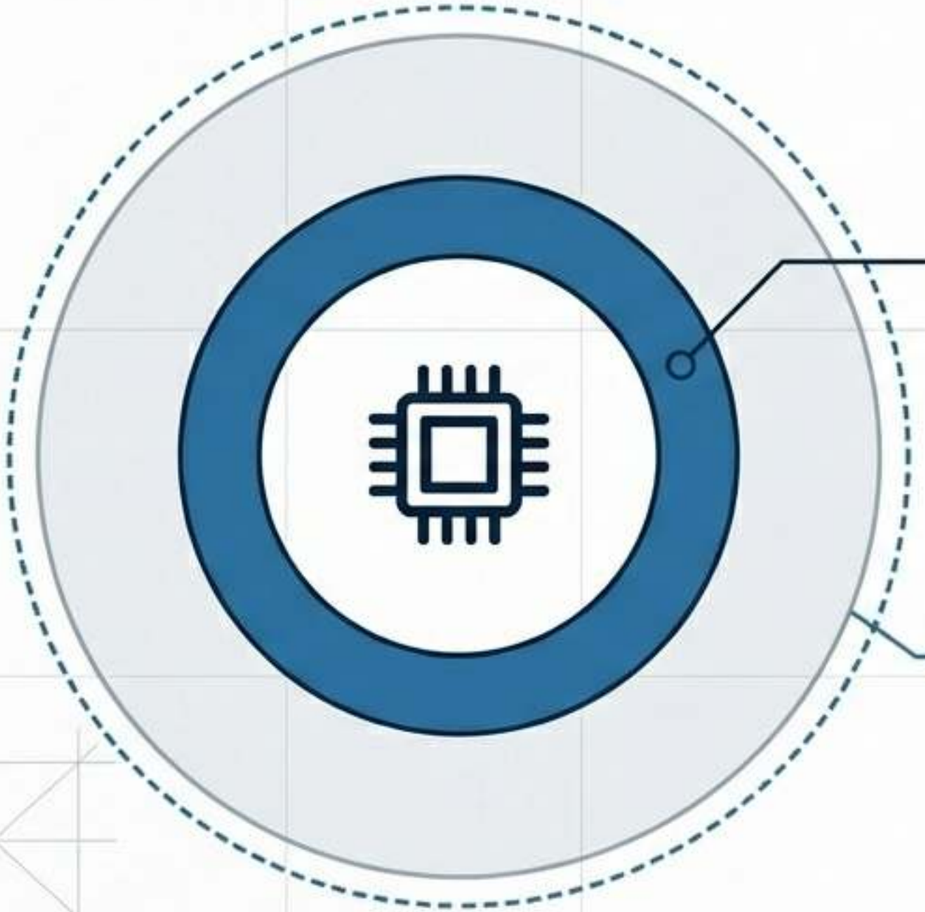
Bias: Documented measures to detect and mitigate algorithmic bias.

Vetted AI Framework

NotebookLM

Pillar 3 validates the human guardrails around the technology

Require evidence of policies and processes, not just verbal assurances.



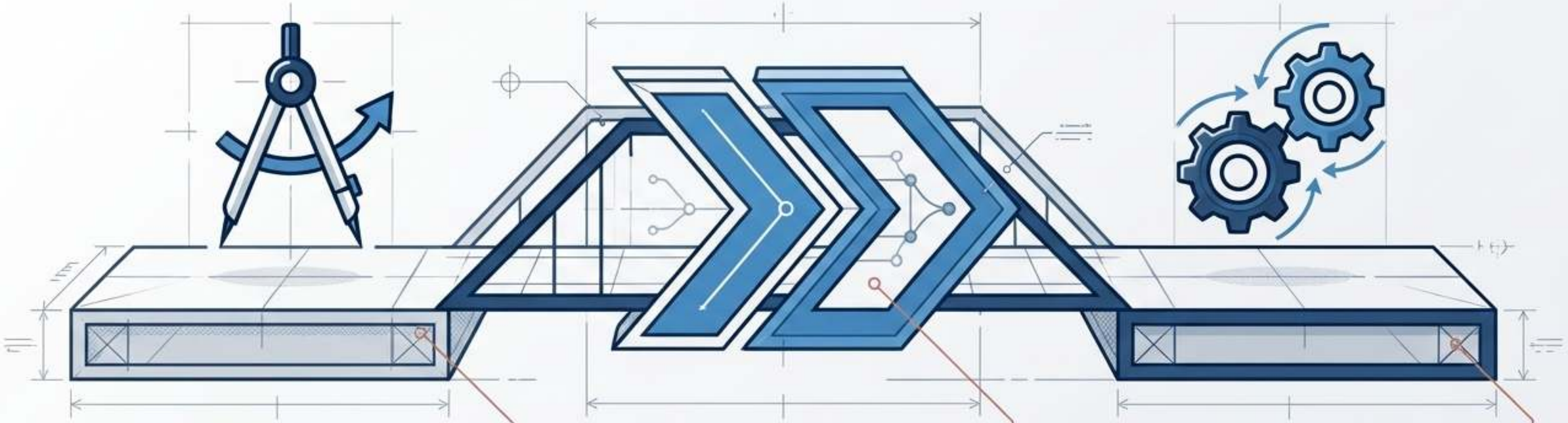
Internal Oversight: Do they have an active ethics board or a responsible AI committee?

External Monitoring: How does the vendor monitor regulatory changes as the legal landscape evolves?

NotebookLM

Pillar 4 measures operational alignment and ongoing support

A robust partnership requires synchronizing roadmaps and integration processes for long-term viability.



Phase 1: Transparency

Evaluate product roadmap transparency.

Alert: Verify access to future product iterations and sunsetting schedules.

Phase 2: Integration

What are the specifific integration requirements and expected enterprise resource commitments?

Critical: Assess API stability, data flow, and required internal engineering hours.

Phase 3: Evolution

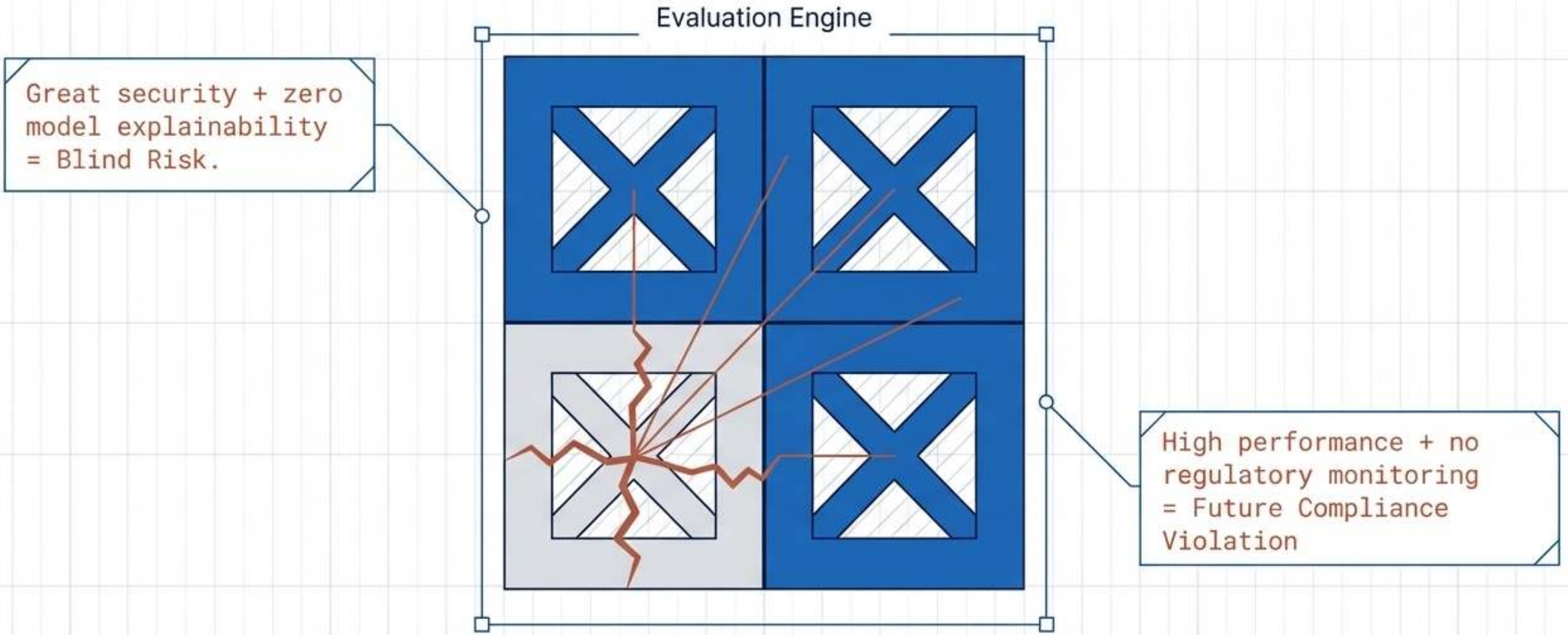
How does their change management process align with yours?

Diagnostic: Review frequency of updates, backward compatibility, and support SLAs.

NotebookLM

A structural failure in any single pillar compromises the entire stack

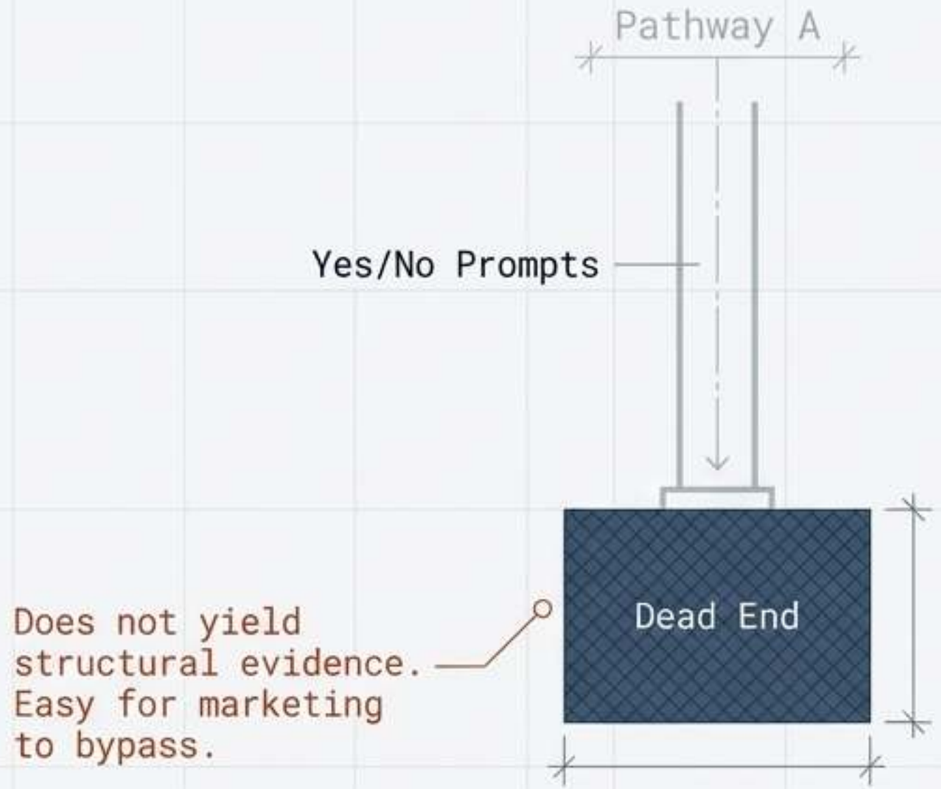
The due diligence questionnaire is a holistic structural test. You cannot compensate for a missing pillar.

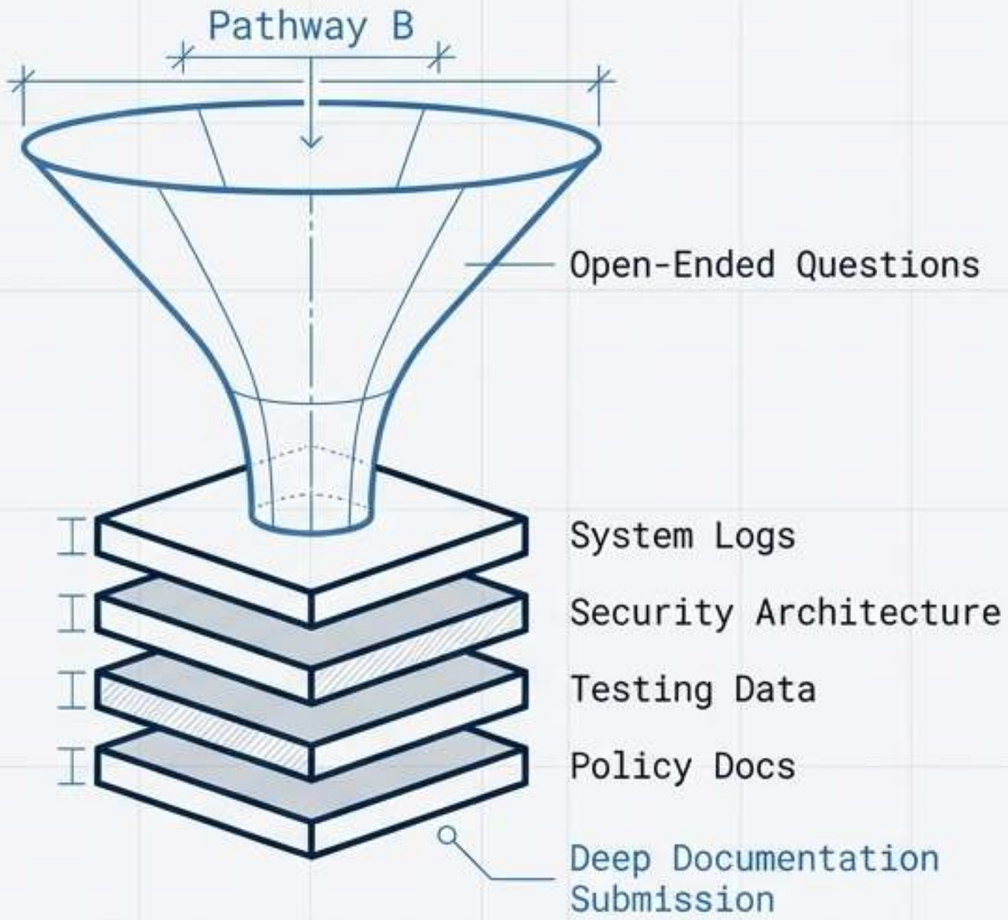


NotebookLM

Force extraction through open-ended inquiry

The depth of a vendor’s answers is itself informative. Frame questions to force the submission of deep documentation.





NotebookLM

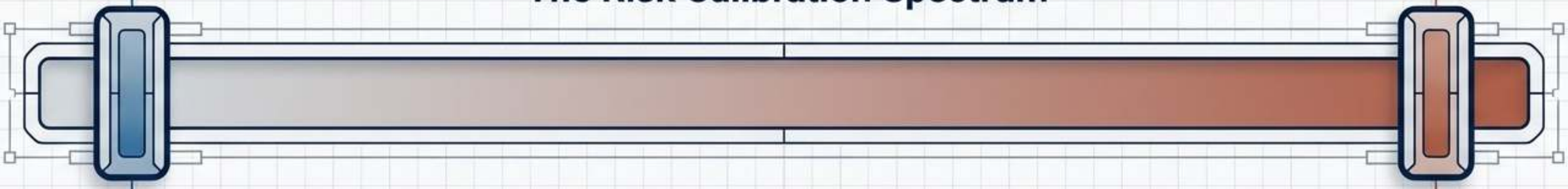
Calibrate the depth of inquiry to the system's risk profile

- Treat the questionnaire as a living document that evolves as regulations change and your risk tolerance adjusts.

Low Risk: Internal summarization tool.

High Risk: Customer-facing financial advisor AI.

The Risk Calibration Spectrum

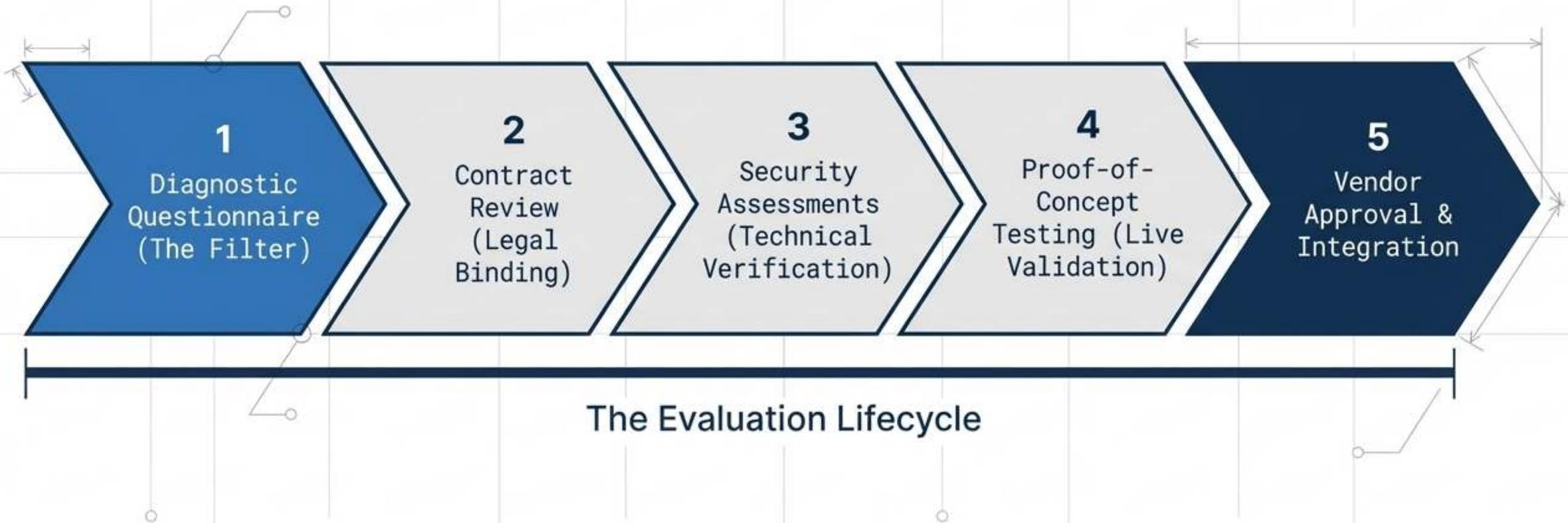


Action: Lighter touch diligence. Focus on basic data retention and access controls.

Action: Exhaustive diligence. Full architectural review, bias testing, and ethics board validation.

NotebookLM

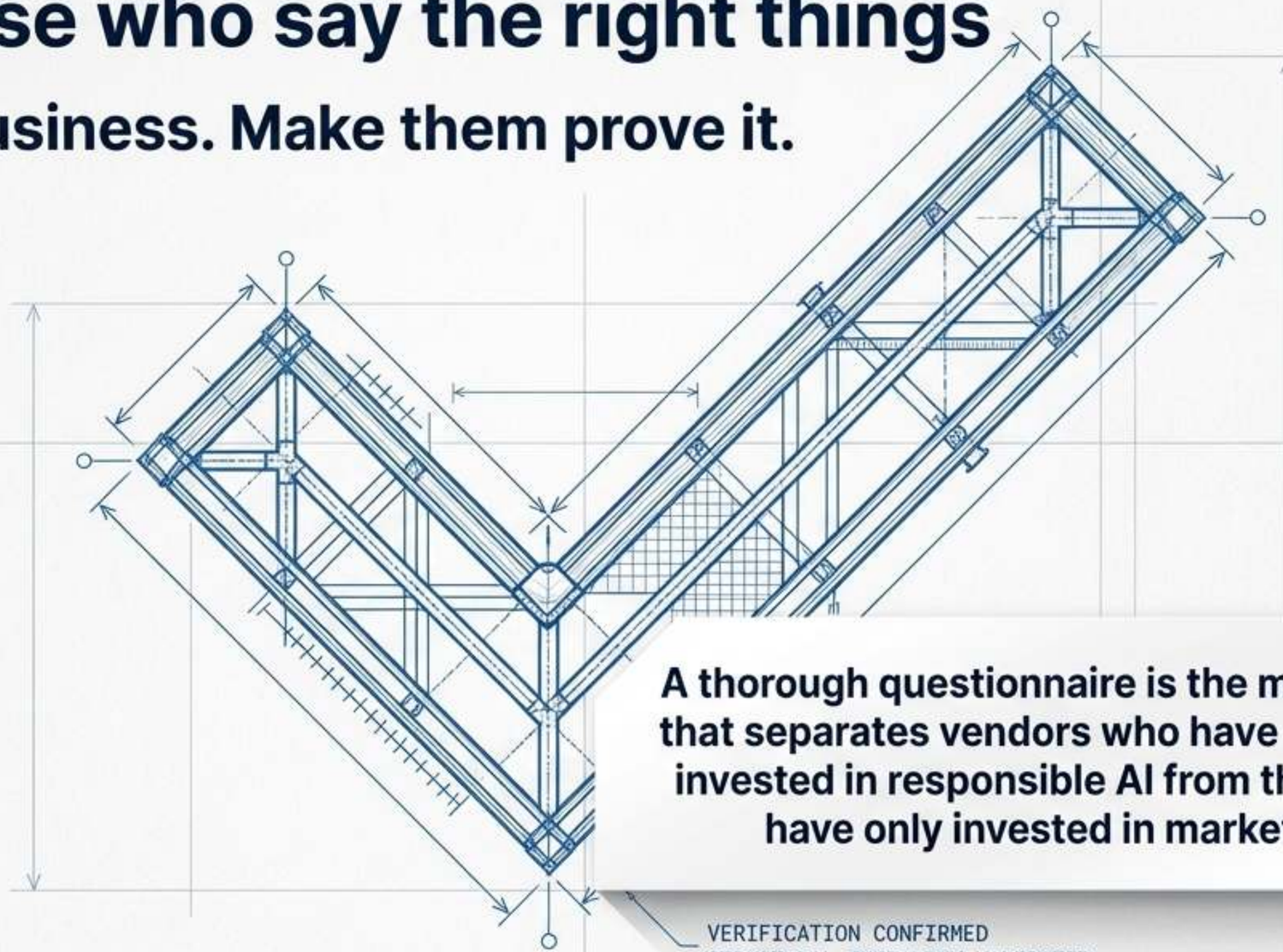
The questionnaire is the first step, not the finish line



NotebookLM

Identify the vendors who do the work, not just those who say the right things

Protect your business. Make them prove it.



A thorough questionnaire is the mechanism that separates vendors who have genuinely invested in responsible AI from those who have only invested in marketing.

VERIFICATION CONFIRMED
STRUCTURAL INTEGRITY VALIDATED

NotebookLM