onetrust

Accelerating innovation with AI-ready governance

October 15, 2025

Today's speakers

Jaimin Patel

Senior Solution Engineer, OneTrust

AI is moving in every direction, fast

Driving a paradigm shift for governance

From

Narrow, predictive applications

Dedicated infrastructure

Specialized teams

To

General purpose systems
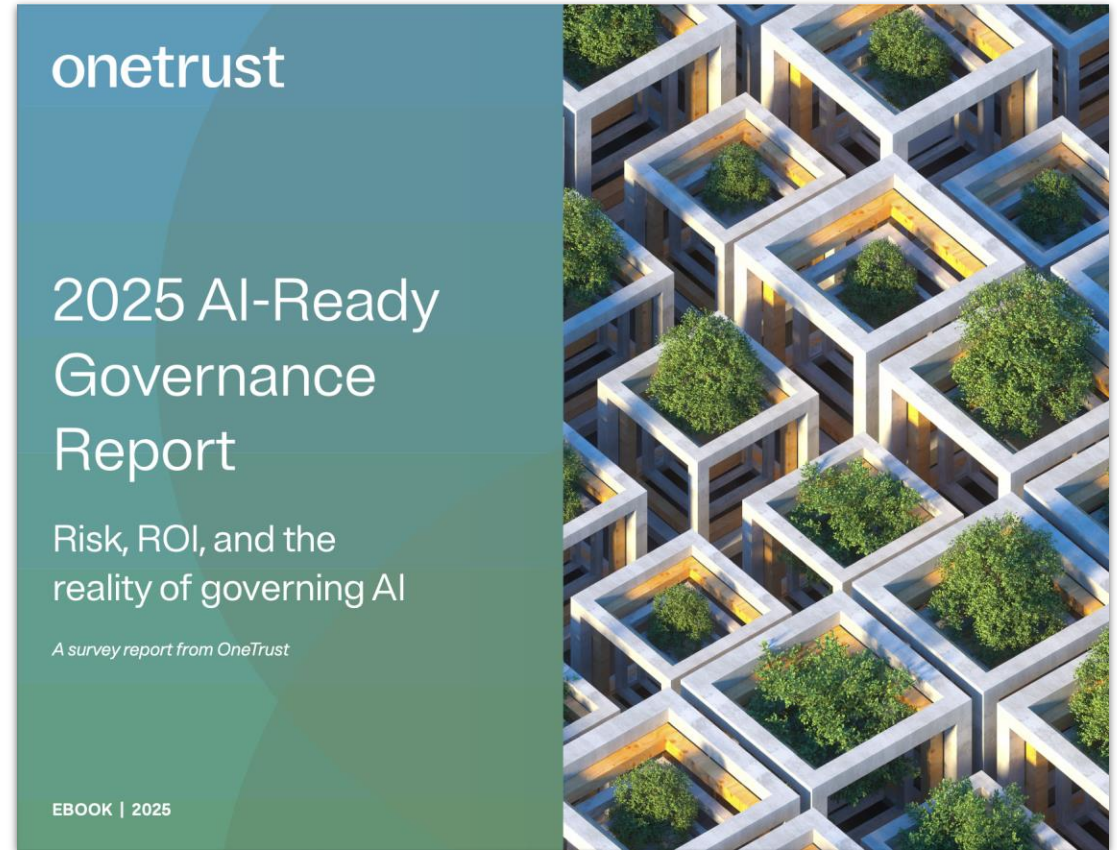
Deeply embedded across tech

Democratized use
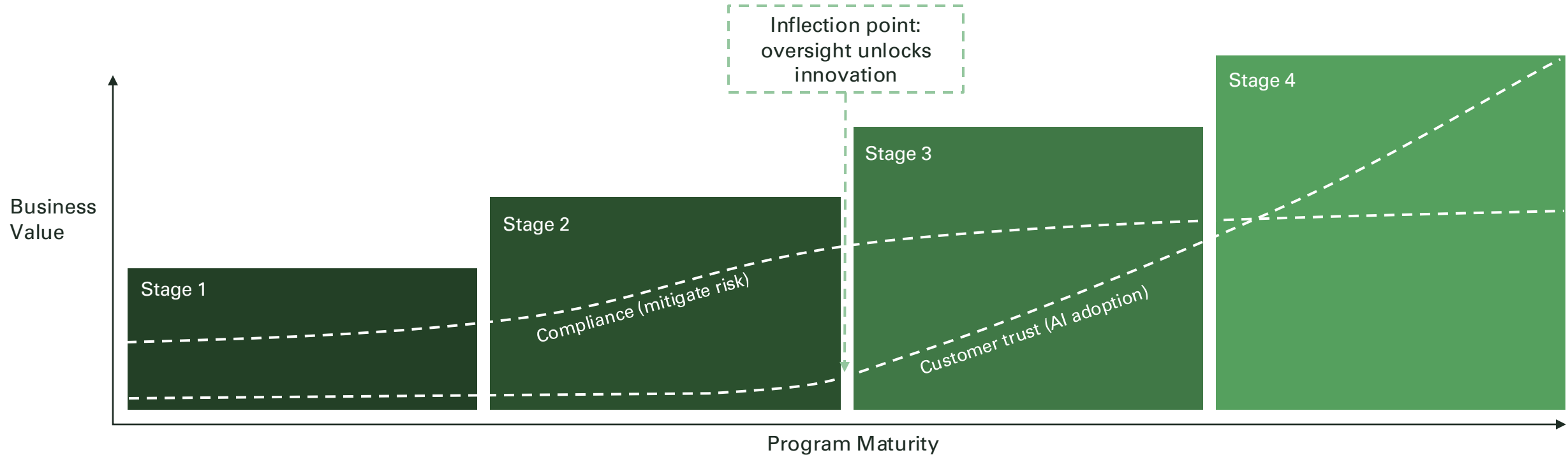
Legacy governance processes can't keep pace

37%
More time managing AI-related risks compared to last year

35%
Cite lack of integration as a challenge for enforcing AI governance at scale

onetrust

2025 AI-Ready Governance Report

Risk, ROI, and the reality of governing AI

A survey report from OneTrust

EBOOK | 2025

The AI Governance Maturity Model

Inflection point: oversight unlocks innovation

Business Value

Stage 1

Stage 2

Stage 3

Stage 4

Compliance (mitigate risk)

Customer trust (AI adoption)

Program Maturity

	Ad Hoc	Defined	Integrated	Scaled
Mindset	Reactive & Compliance Driven	Proactive & Compliance Driven	Embedded into AI lifecycle	Governance Unlocks Value
Org Alignment	Fragmented & constrained	Complex, siloed, manual	Structured, strategic	Scaled across the business
Tech Focus	Inventory establishment	Operationalizing standards	AI ecosystem integration	Run-time enforcement

Requirements depend on risk
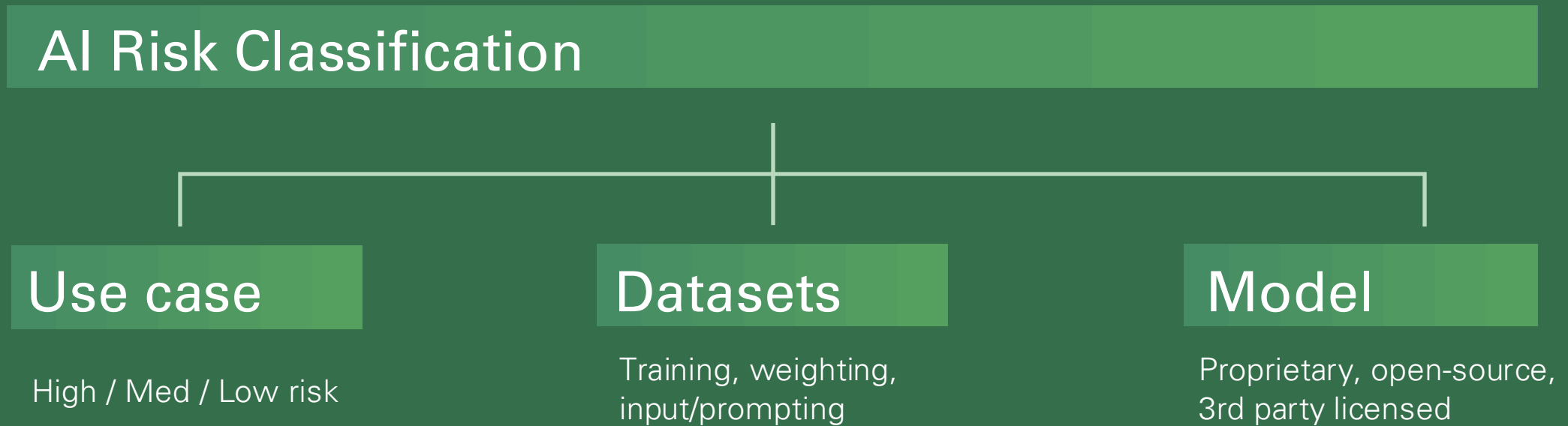
AI Use Case Intake → Initial risk evaluation

Risk vs. ROI

Low risk "fast-track"
- Documentation
- Transparency
- Monitoring

Medium risk guardrails
- Risk acceptance & attestation
- Documentation
- Transparency
- Monitoring

High risk guardrails
- Enhanced due-diligence
- Executive committee review
- Risk acceptance & attestation
- Documentation
- Transparency
- Monitoring

Unacceptable risk
- Reject

Operationalize workflows to align with levels of risk and impact

Effective intake captures context

AI Risk Classification

Use case

High / Med / Low risk

Datasets

Training, weighting, input/prompting

Model

Proprietary, open-source, 3rd party licensed

Effective intake captures context

AI Risk Classification

Use case

High / Med / Low risk

- Project management
- IT ticketing
- Spreadsheets

Datasets

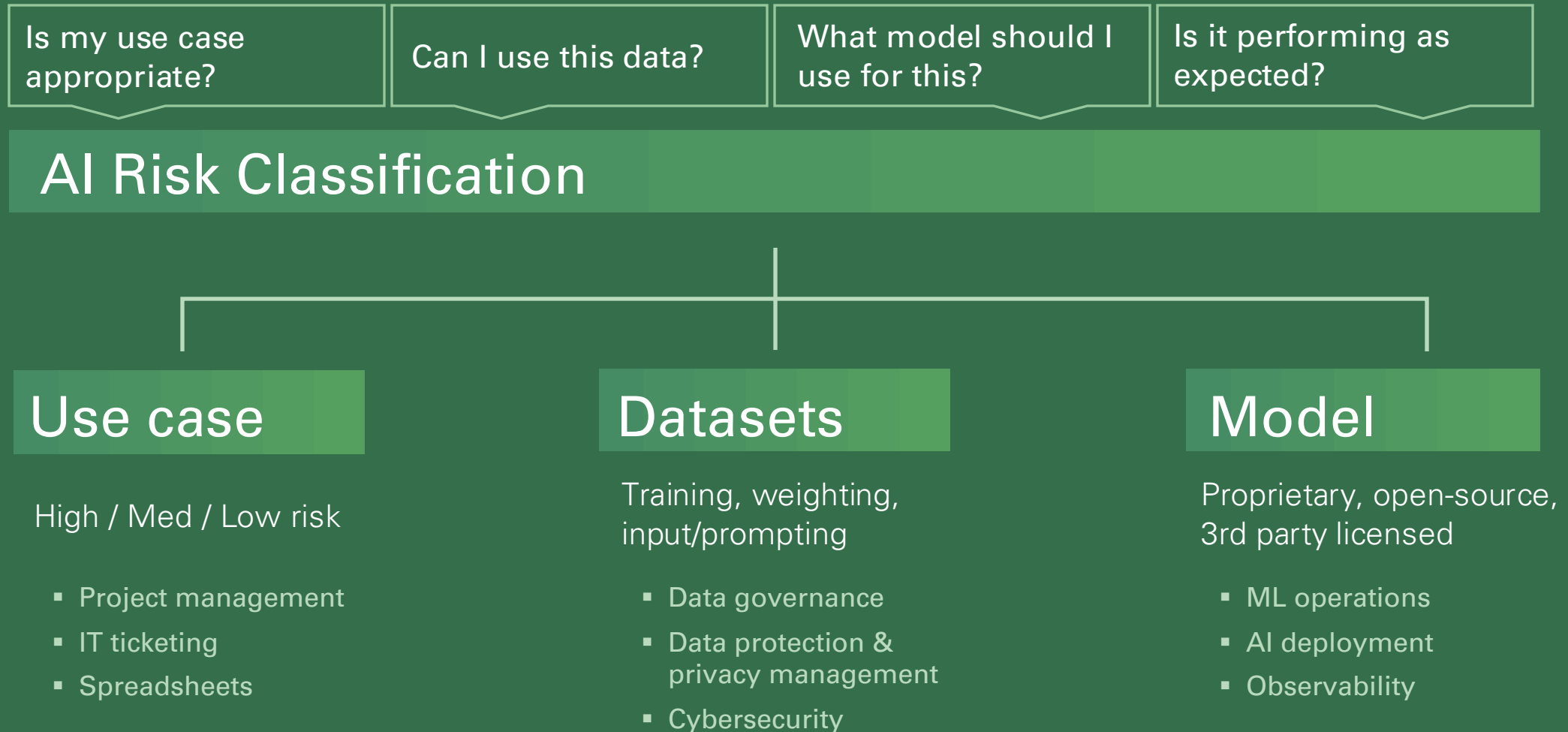Training, weighting, input/prompting

- Data platforms
- Privacy management
- Cybersecurity

Model

Proprietary, open-source, 3rd party licensed

- ML operations
- AI deployment
- Observability

Committees need a system to evaluate context at scale

| Is my use case appropriate? | Can I use this data? | What model should I use for this? | Is it performing as expected? |

AI Risk Classification

Use case

High / Med / Low risk

- Project management
- IT ticketing
- Spreadsheets

Datasets

Training, weighting, input/prompting

- Data governance
- Data protection & privacy management
- Cybersecurity

Model

Proprietary, open-source, 3rd party licensed

- ML operations
- AI deployment
- Observability

The AI Governance stack

No single layer is sufficient; effective governance spans people, process, and systems

Governance layer		Jobs to be done	Stakeholders
Risk & Compliance		Define AI risks and acceptable use Ensure full coverage of AI use (built, bought) Enforce policy, approvals, and accountability Demonstrate compliance	AI Governance steerco (x-functional) AI Governance officers Privacy, Compliance, Risk officers Legal / privacy / policy teams
Observability		Understand and monitor AI behavior / performance Manage the AI lifecycle across systems	ML & Data Product Managers Model developers & evaluators Platform owners
Enforcement		Integrate runtime guardrails Manage technical risk pre-/post-deployment	Data platform & infra engineering Enterprise architects Data stewards
Data & AI Platforms	Systems of Record	Govern access to data, features, and AI artifacts across environments Deploy into production securely & efficiently Configure and adopt AI Enforce cost controls, resource entitlements	IT Enterprise architects Business owners / analysts

The AI Governance stack
Governance must evolve with AI, not lag behind it

Risk & Compliance
Observability
Enforcement

| Data & AI Platforms	Systems of Record
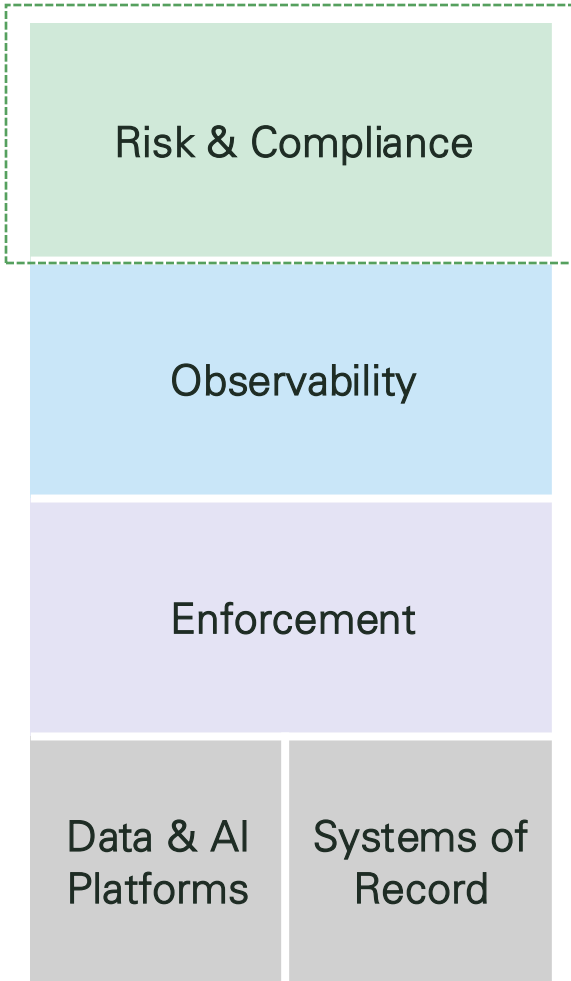
Challenges:
- Disconnected from AI behavior and state
- Manual workflows increase overhead
- Documentation is stale without runtime context

The AI Governance stack

Effective governance is not limited to model monitoring in isolation, undocumented decisions,and unprioritized issues

Risk & Compliance

Observability

Enforcement

Data & AI Platforms

Systems of Record
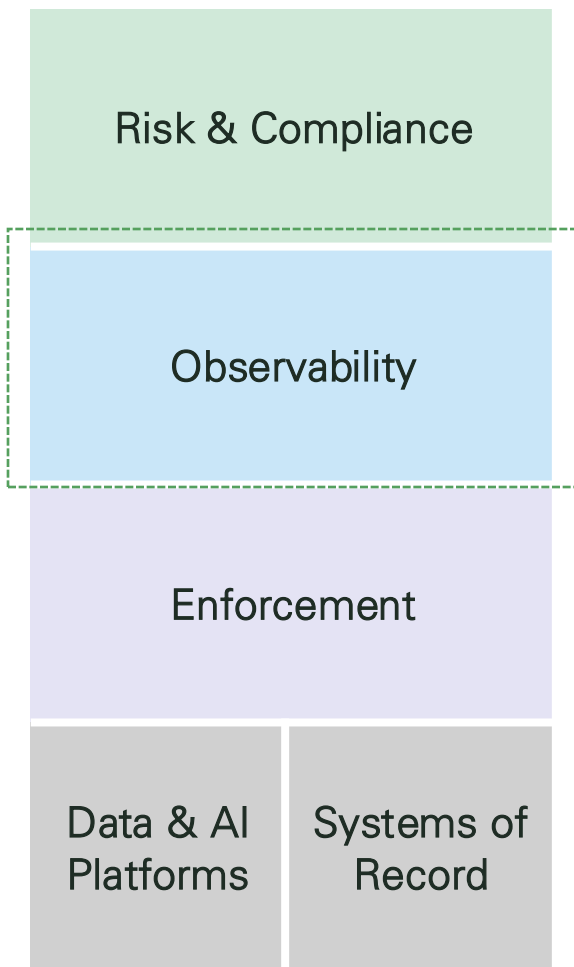
Challenges:
- Business risk not reflected in model management
- Siloed tools for drift, bias, and lineage create visibility gaps
- No feedback with compliance and risk owners
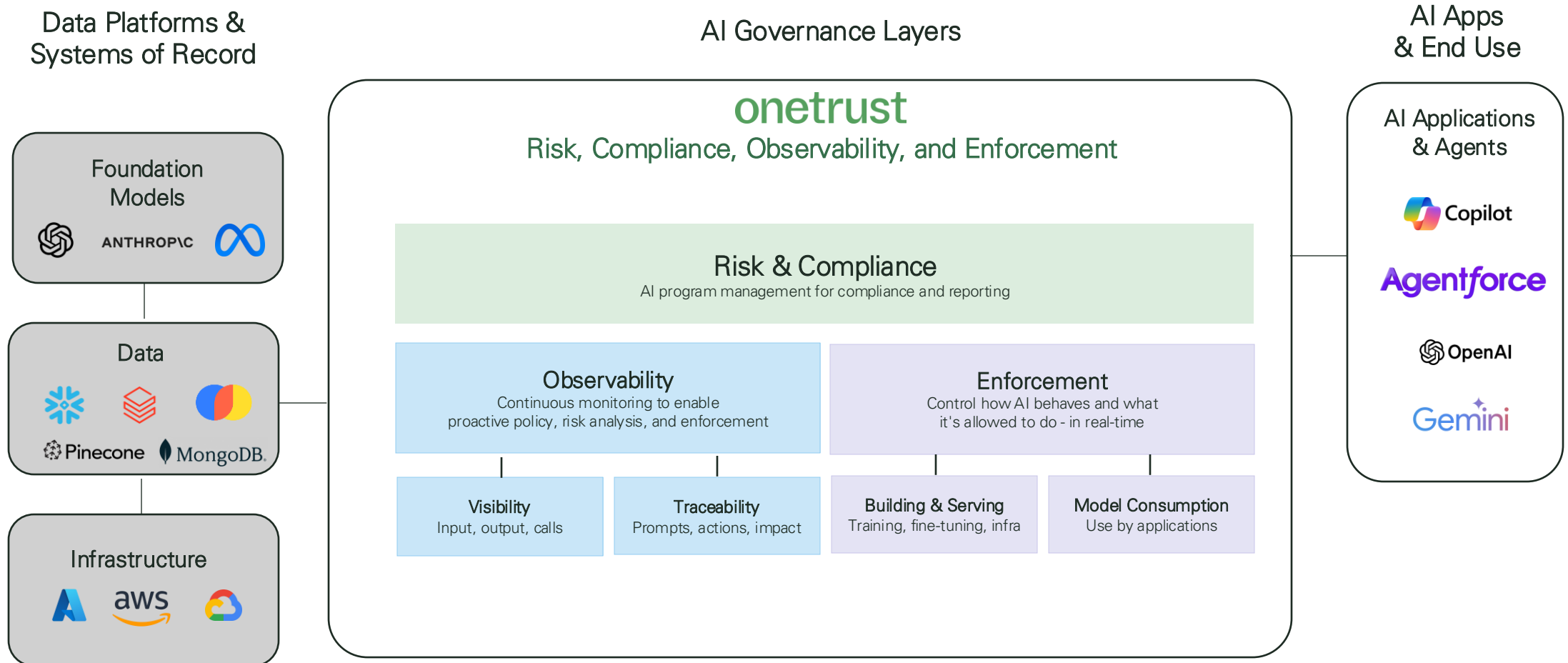
The AI Governance stack
AI is built, deployed, and embedded everywhere—often without oversight

Risk & Compliance

Observability

Enforcement

Data & AI Platforms

Systems of Record
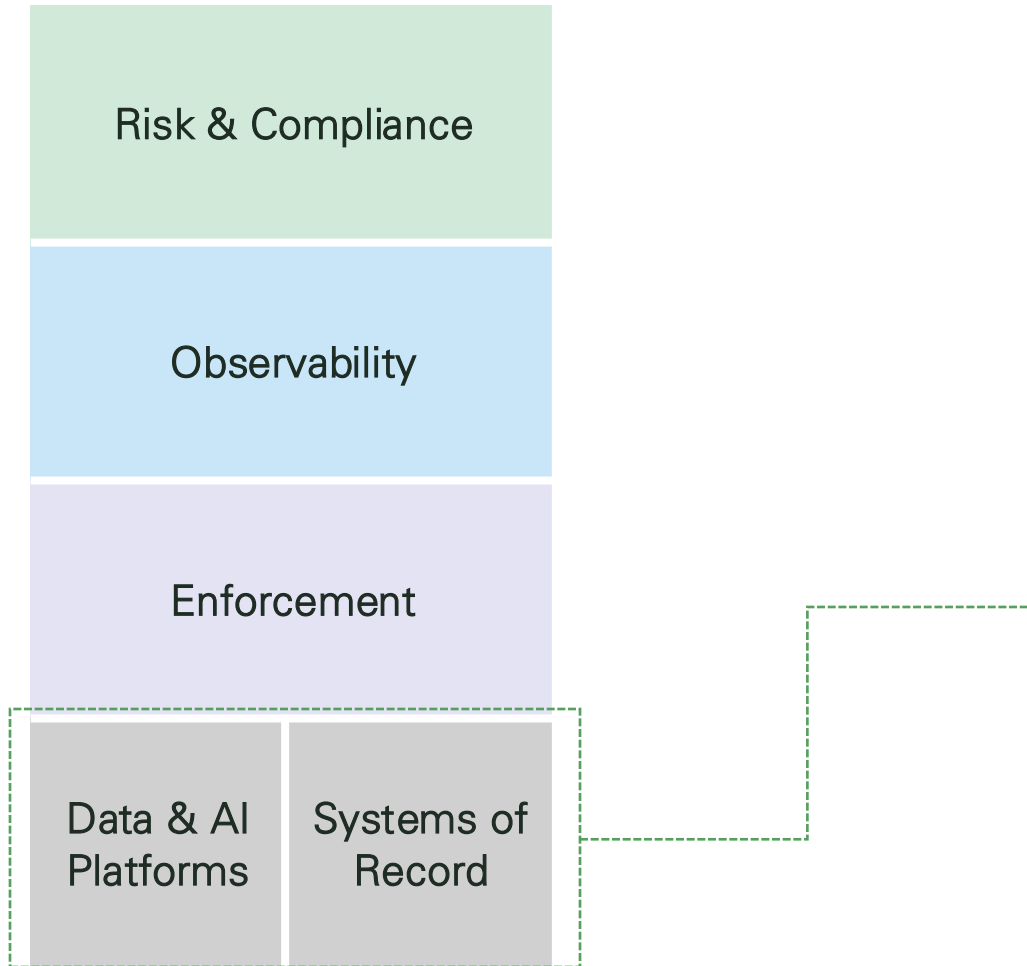
Challenges:
- AI adoption outpaces governance coverage
- Accountability is limited to resource management
- No ties to risk, policies, and compliance

The Data & AI Control Plane for Continuous AI Governance

Data Platforms & Systems of Record

Foundation Models

Data

Infrastructure

AI Governance Layers

onetrust
Risk, Compliance, Observability, and Enforcement

Risk & Compliance
AI program management for compliance and reporting

Observability
Continuous monitoring to enable proactive policy, risk analysis, and enforcement

Visibility
Input, output, calls

Traceability
Prompts, actions, impact

Enforcement
Control how AI behaves and what it's allowed to do - in real-time

Building & Serving
Training, fine-tuning, infra

Model Consumption
Use by applications

AI Apps & End Use

AI Applications & Agents

Copilot

Agentforce

OpenAI

Gemini

Demo