

DRATA

Put Security and
Compliance on
Autopilot

AI & Machine Learning

Lior Solomon

Pratik Bhat



Meet our presenters



Lior Salomon
VP of Data Engineering

DRATA



Pratik Bhat
AI Product Manager

DRATA



Today we'll discuss

1. Why AI? Why now?
2. AI Strategy Framework
3. Building Trust with Customers
4. AI Product Development Process
5. AI Use Case: Security Questionnaires
6. AI Evals

Drata: On a Mission to Build Trust Across the Cloud



\$328M

Total Funding

ICONIQ



COWBOY
VENTURES

Notable.

ALKEON
CAPITAL MANAGEMENT

The #1

Compliance Partner

- ✓ 20+ compliance frameworks
- ✓ 200+ integrations
- ✓ Automated evidence collection
- ✓ Continuous control monitoring

5,000+

Customers



Trust Center/Reports



Third Party Risk Management



Continuous Control Monitoring



User Access Reviews



Internal Risk Management



+ more

Why AI?

Why should we care about AI / ML advancements today?



Unstructured text

Enterprise data is primarily unstructured text. LLMs are amazing at understanding and generating it.



Cost of development

Every year the cost of using and deploying models is rapidly decreasing.



New user experiences

Reasoning and deep natural language understanding can empower GRC teams with better automation while reducing cognitive load

AI Strategy Framework

Aligned AI Vision

Align your AI to your organization's broader mission, vision, and growth strategy.

➤ Focused on:

Strategic alignment with company OKRs and business objectives

Ethics + Governance

Create your AI governance approach to define how you'll use AI ethically and mitigate risk.

➤ Focused on:

Transparent communication within organization and to customers

Opportunity Identification

Identify AI opportunities for productivity gains and organizational transformation.

➤ Focused on:

Low-risk projects driving quick customer impact and trust

Roadmap & Goals

Prioritize your AI opportunities and build a roadmap supported by goals/OKRs.

➤ Focused on:

Try and align with existing product roadmaps to support existing goals

Organization Enablement

Consider how you'll re-skill your team, structure your organization, and organize your data.

➤ Focused on:

Identify relevant skilled engineers and reduce dependencies

How to build trust with customers while exploring this new technology



Privacy by Design

Data anonymization and separation with strict access controls and encryption protocols



Fairness & Inclusivity

Monitoring model outcomes for bias and harmful outputs.



Safety & Reliability

Rigorous testing with comprehensive evals including synthetic data



Human in the loop

Our internal security and GRC team are always involved throughout the product life cycle

AI Product Development Process

Ideation

High Level User Journey: Mapping the E2E user experience and uncovering constraints of a proposed solution.

Data Journey: Mapping the entire data journey – What data is sent to the AI service? What is the expected output?

Validation

Build a functional E2E POC to validate feasibility of the project and provide feedback.

Refine the project goals and scope based on the feedback.

Prioritization

We will prioritize projects across various factors including customer value & reach, business impact, differentiation, effort, and more.

The POC helps us understand whether an AI enabled solution is the right fit for the problem.

Internal Testing

An internal council at Drata consisting of our GRC experts, security & compliance team, and leadership members review EVERY project.

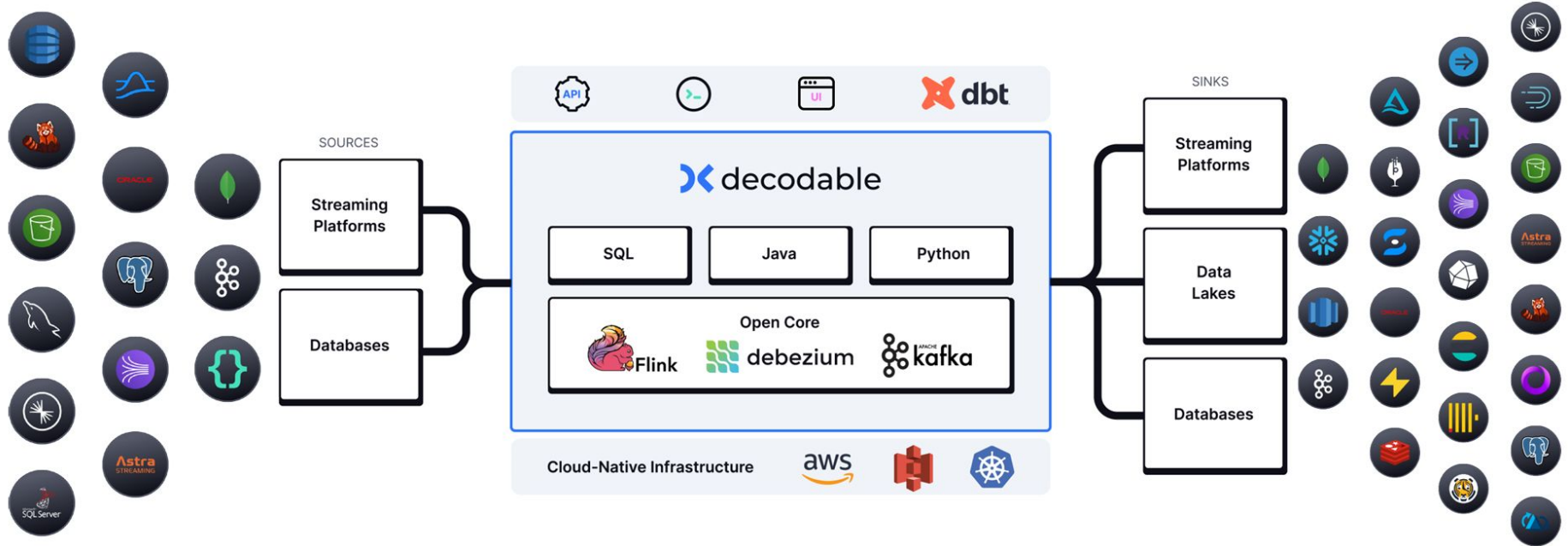
Combining automated testing methods with human reviews.



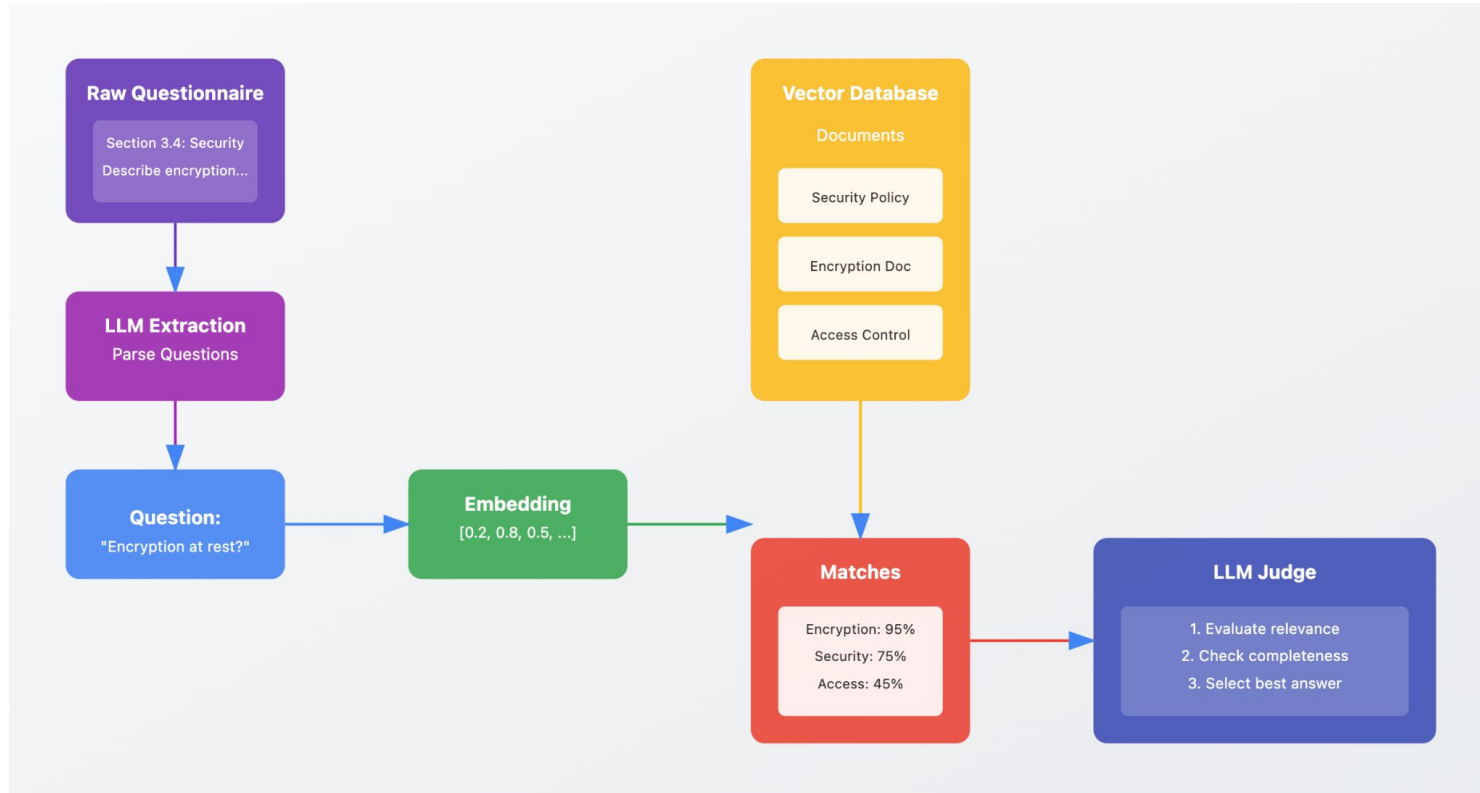
AI Use Case: Security Questionnaire

- **Challenge:** Security questionnaires are time-consuming and impact critical business processes.
- **AI Solution:** AI-driven questionnaire agent automates responses using **LLM** (Large Language Model) and **RAG** (Retrieval-Augmented Generation) knowledge base application.
- **Observability:** Monitors data quality scores, tracks schema changes, and ensures data freshness.
- **Benefits:** Reduces response time from days to minutes, improves accuracy, and enhances customer experience.

Radically Simplifying Real-time Data for All

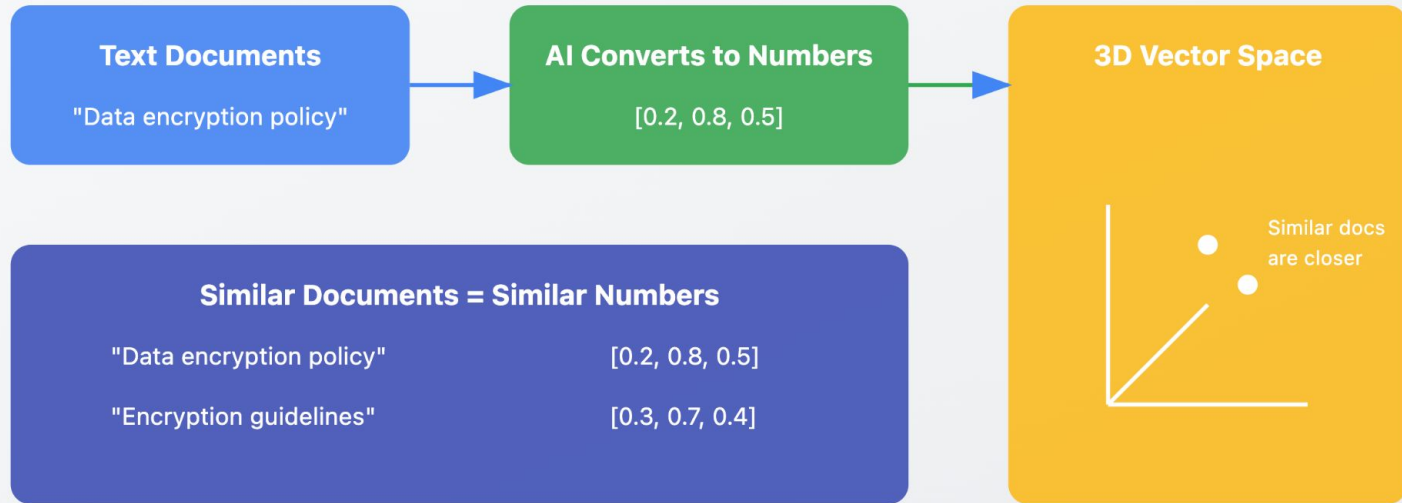


RAG Architecture



Embedding

Understanding Document Embeddings



Documents with similar meaning have similar number patterns, making them easy to find

AI Evals

How to evaluate AI outputs across a variety of metrics



Relevance Scoring

Evaluate response quality through semantic similarity scoring, context-awareness assessment



Source Verification

Validate responses against the knowledge base through document citation tracking.



LLM as Judge

Leverage additional language models to assess response quality, perform cross-validation, and ensure consistency.



Knowledge Base Completion

Monitor document freshness, perform regular content gap analysis, and ensure version control for customer-provided security documentation.



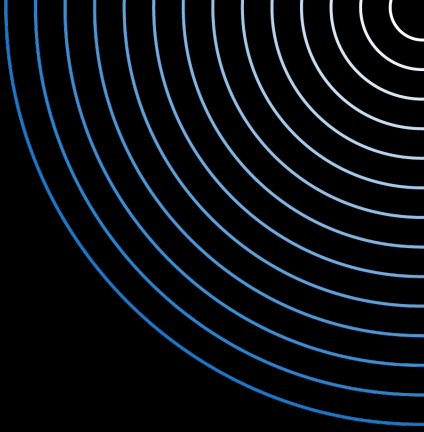
Human Validation Pipeline

Implement systematic expert review sampling and feedback integration to continuously improve the system's accuracy and reliability.



Future of Drata AI

*"Make GRC more effortless,
accessible, and automated than
ever before."*



Q&A