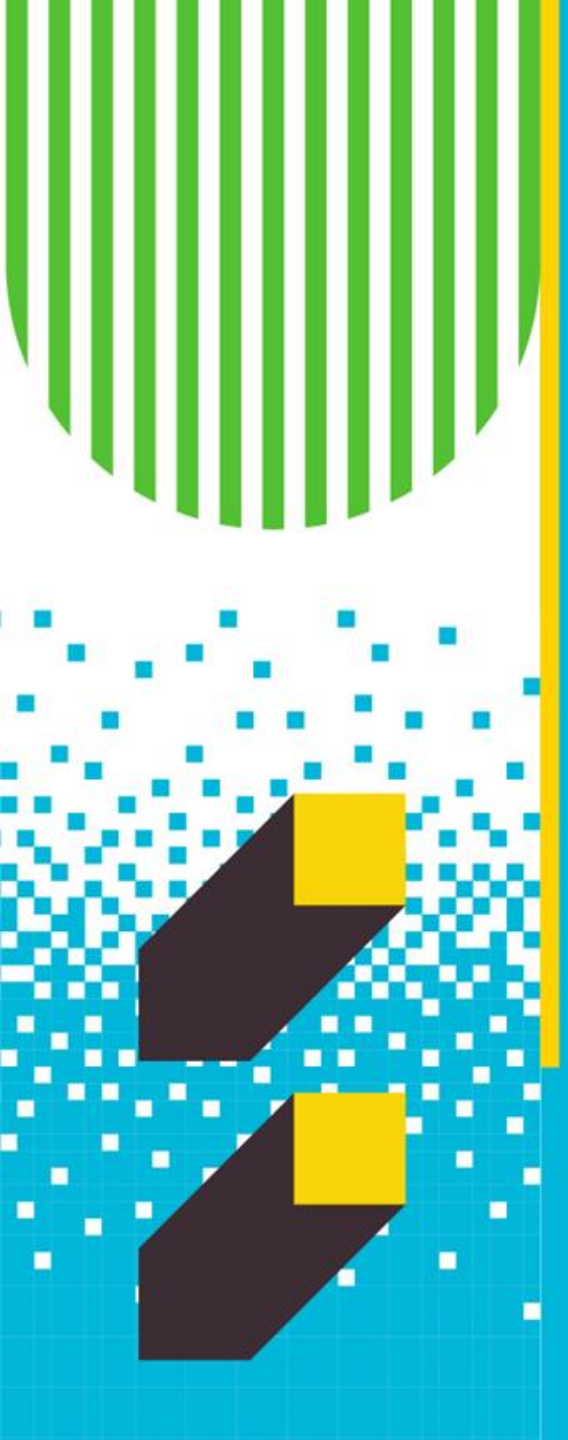


IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

Jessica Pate

Data privacy, my favorite problem to solve

Head of Privacy Expert relyanceai

Today's Panelists

Heather
Allen

CHG Healthcare

Sheila
Jambekar

dayforce

Today's Session

The Challenge

AI Agents are rising, and risks are compounding

The Rewiring of Mindset

Adapting our mindset for autonomous AI systems

The Framework

The governance playbook for AI Agents, with lineage at the core

Live Demo

Putting the governance framework into practice – live

Your Data Defense Engineer

From Code-to-Cloud

relyanceai

The State of Enterprise Agentic AI

Unlock

79%

They have some form of adoption of AI agents

Source - PWC AI Agents reports

88%

Plan to increase AI Budget driven by AI agent adoption

Source - PWC AI Agents reports

Blind Spots

$412M

2024 US regulatory settlement due to AI Security related Incidents

Source - IBM Cost of Data breach report

63%

Breached organizations don't have an AI governance policy

Source - IBM Cost of Data breach report

60% of AI incidents led to data compromise, 31% to operational disruption

Source - IBM 2025 Cost of a Data Breach Report: PWC AI Agents reports

"We are now confident we know how to build AGI as we have traditionally understood it. We believe that, in 2025, we may see the first AI agents join the workforce and materially change the output of companies"

- Sam Altman

relyanceai

Agentic AI is inevitable.
The choice is not whether we will use it,
but how responsibly we will adopt it

From Rules to Self-Direction: Compounding AI Risks

Traditional AI

Executes fixed tasks – reliable but narrow
Uses structured data – limited input scope
Deterministic rules – predictable, inflexible

Governance Risk

Bias in encoded rules
Opaque decision processes

Security Risk

Rule bypass exploits
Data drift failures

Generative AI

New outputs – from unstructured data
Learns patterns & behaviors – beyond rules
Context-aware reasoning – probabilistic

Governance Risk

Training data misuse
Unexplainable model outputs

Security Risk

Sensitive data leakage
Prompt injection attacks

Agentic AI

Interprets intent – converts goals to plans
Chains actions – executes across systems
Autonomous – adaptive, fewer touchpoints

Governance Risk

Accountability void
Opaque reasoning chains

Security Risk

Cascading system failures
Privilege and identity misuse

AGI

Self-reflection – learns from past actions
Transfer learning – adapts across domains
Open-ended goals – self-directed objectives

Governance Risk

Oversight collapse
Unbounded machine decisions

Security Risk

Emergent unpredictable behaviors
Autonomous misuse at scale

Rule — Behavior — Intent — Autonomy — Self-reflection — Self-direction

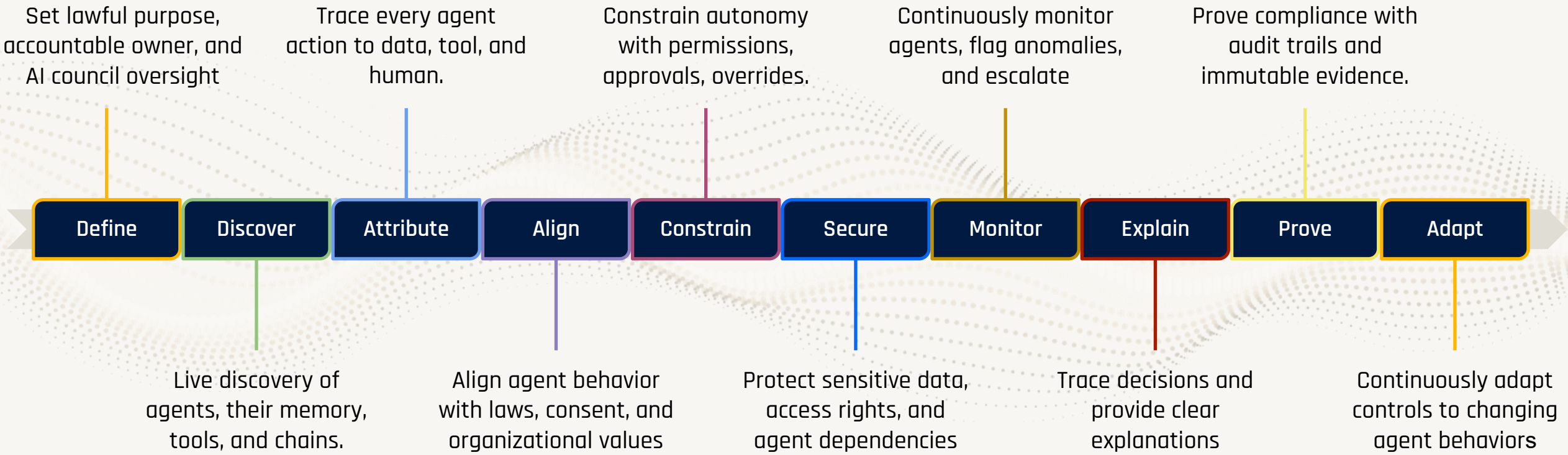
relyanceai

As AI risks compound, our mindset for Governing and Securing AI applications must evolve

relyanceai

10 Stage AI Governance Framework

The Agentic AI Governance Framework → *Autonomy to Accountability*



relyanceai

From Framework to Frontline
Making it Real in Practice

Discover

Business Outcome

Full visibility into all sanctioned and shadow agents

Proactively spot consent and **privacy blind spots.**

Build a **reliable digital map of every system**, including its inputs, outputs, and the sensitive data it interacts with.

Jobs To Be Done

Inventory all agents with their memory, tools, and task chains

Detect shadow agents operating outside sanctioned systems

Map data flows and dependencies touched by each agent

Continuously update inventory – not a one-off exercise

Key Metric

Shadow Agent Detection Rate
% of rogue/unsanctioned agents identified over a given time.

AAC - Accountable Agent Coverage
% of agents that are discovered, registered, and tied to a human owner with a defined purpose

Business Outcome

Prevent agents from exceeding approved authority

Reduce liability from high-risk or unauthorized actions

Ensure humans retain final decision rights

Jobs To Be Done

Define agent permissions and escalation thresholds

I**mplement** human approvals for high-risk actions

Establish kill switches and override controls

Apply tiered autonomy – expand only when proven safe

Key Metric

UAR – Unauthorized Action Rate
% of actions beyond granted scope

HEP – Human Escalation Precision
accuracy of escalations vs false positives

Business Outcome

Protect sensitive data from misuse or leakage

Prevent unauthorized access to tools and systems

Ensure resilience against adversarial attacks and exploits

Jobs To Be Done

Enforce least-privilege and zero-trust access for agents

Protect sensitive data lineage across memory and tools

Test resilience through adversarial probes and red teaming

Secure agent dependencies (APIs, plugins, external services)

Key Metric

SDLE – Sensitive Data Lineage Exposure
% of data flows untracked or unsecured

PSE – Prompt Shield Effectiveness
% of injection/jailbreak attempts blocked

Data Lineage: The Crown Jewel of Agentic AI Governance

10 Stage Agentic AI Governance Framework

Context-aware *Data Lineage*

Data lineage enables compliance with EU AI Act, ISO 42001, and NIST AI RMF.

Data lineage exposes shadow agent call chains, sensitive data flows, and agent overreach.

Data lineage provides accountability through audit trails of data, prompts, and actions.

Data lineage strengthens security by tracing leaks, privilege abuse, and cross-system cascades.

Data lineage builds trust with explainable and defensible AI outcomes

relyanceai

What if.....

AI Agent(s)

Automate | Operationalize

JOBS TO BE DONE

10 Stage Agentic AI Governance Framework

relyanceai

Meet Your Data Defense Engineer

From Code-to-Cloud

✦ Ask Your Data Defense Engineer

ai Privacy Expert | ai Data Security | ai AI Governance Expert

Automate | Operationalize

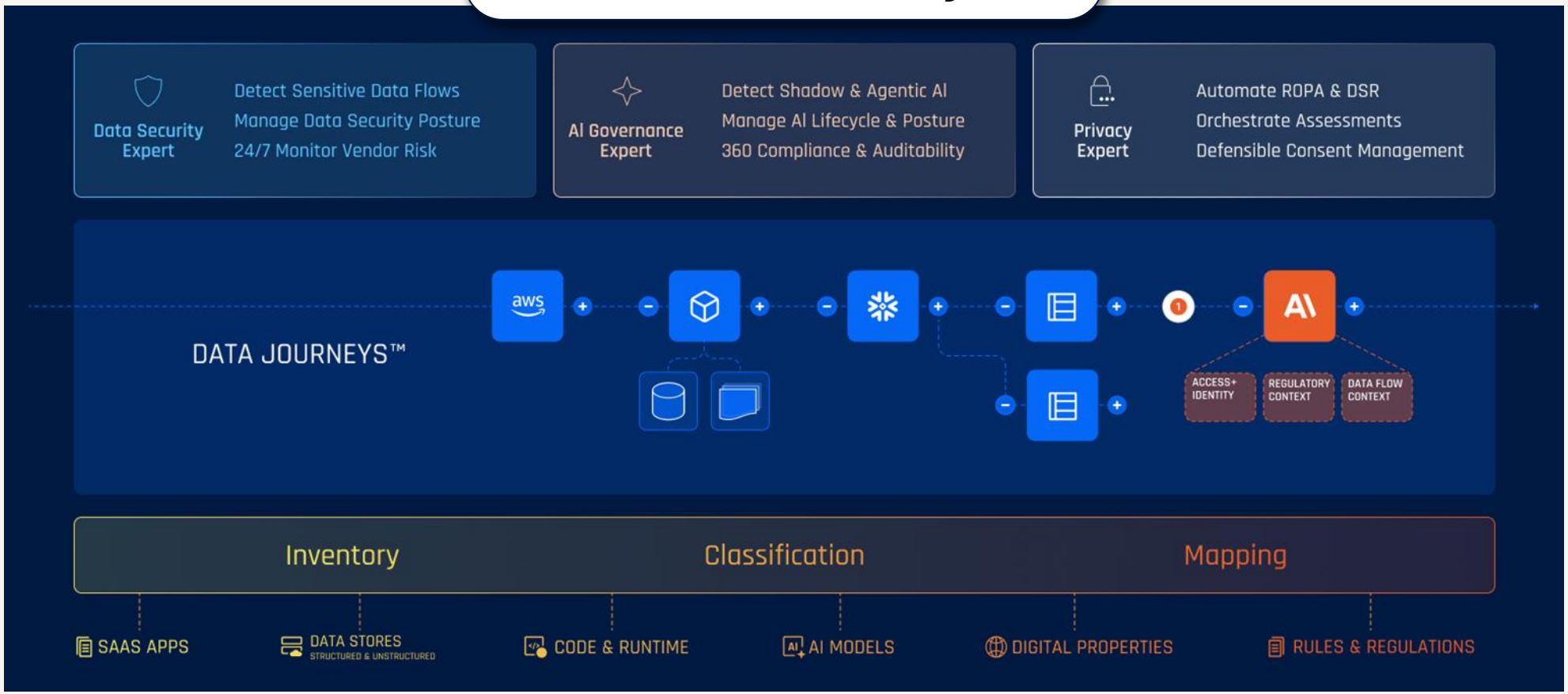
JOBS TO BE DONE

10 Stage Agentic AI Governance Framework

Complete. AI-Native. Unified

Complete code-to-cloud data lineage, AI-native security controls, and unified governance in one agentless platform

✦ Ask Your Data Defense Engineer



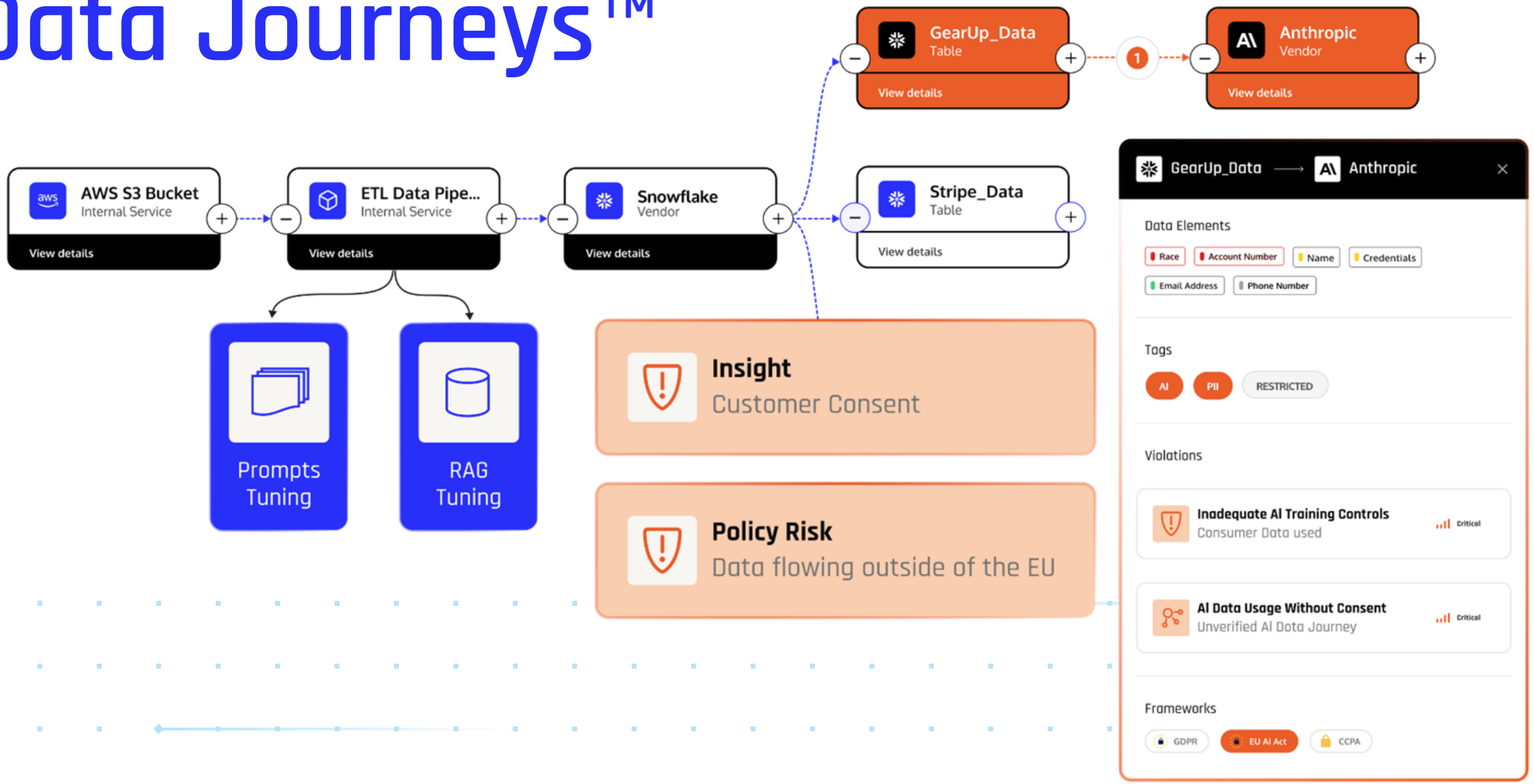
Integration-First Approach

CI/CD pipelines : Cloud platforms : Security tools : Data platforms

Deployment Options That Fit Your Architecture

Full SaaS, InHost™, DirectConnect

Context-Aware
Data Journeys™



Purpose Validation

Data Journeys™

relyanceai

Q & A

relyanceai

Free Resource!

“The Agentic AI Governance Playbook”

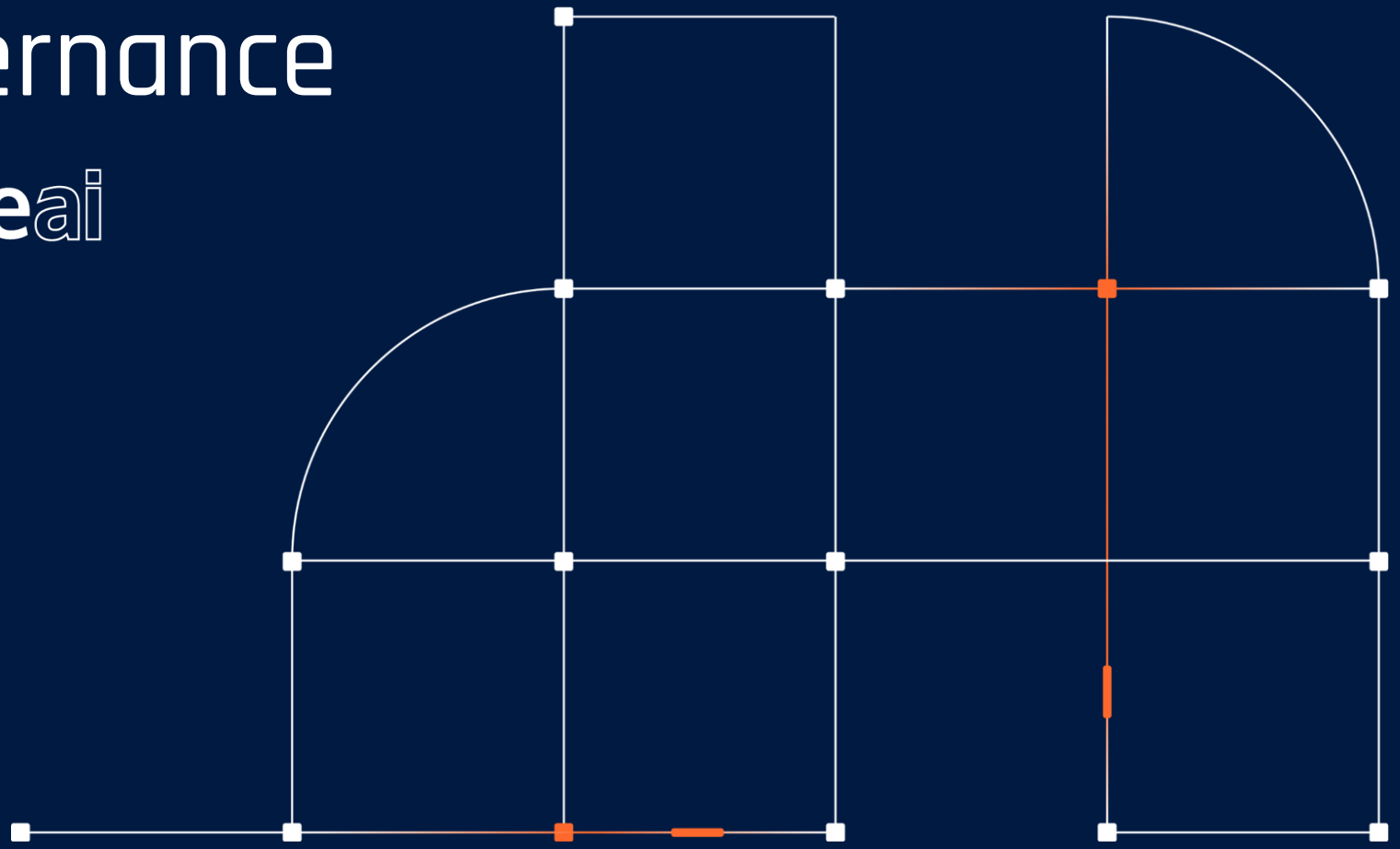
or email at

jessica.pate@relyance.ai

relyanceai

Take your first steps toward AI Governance with relyanceai

Booth #213



How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!