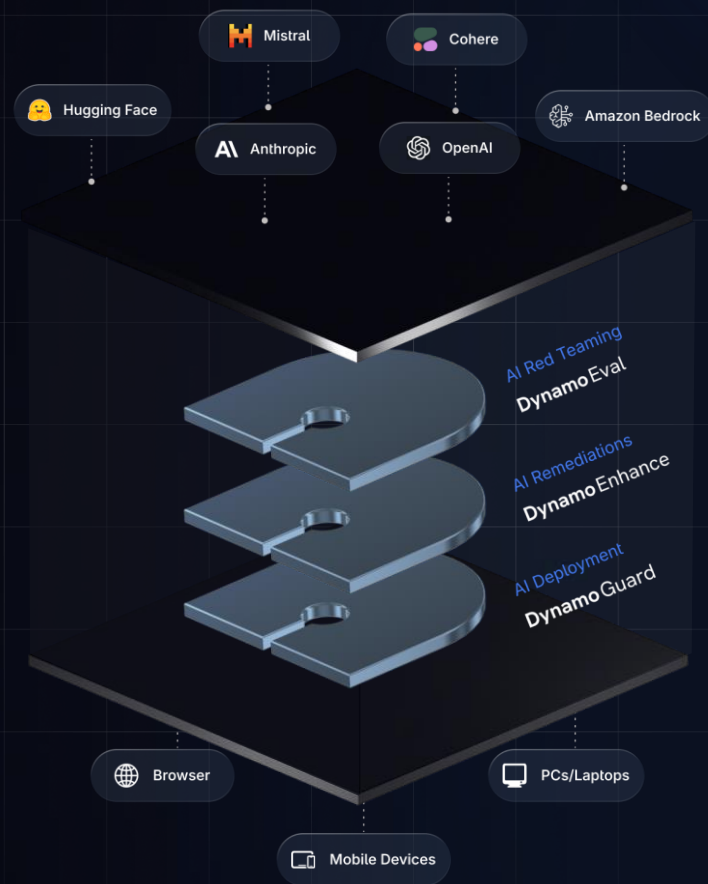# Dynamo AI

Engagement Support Model

Outline

☑ **Engagement and Support Model Overview**

☑ **Operating Model Deep Dive**

☑ Engagement and Support Model Overview

Dynamo AI Delivery

Dynamo provides a comprehensive platform for highly-regulated enterprises to streamline Gen AI system red-teaming, model control application, compliance documentation, and ongoing monitoring.

Dynamo includes:

1. **Automated red-teaming** for stress-testing of Gen AI-based applications against emerging prompt injection and jailbreaking vulnerabilities and hallucinations.

2. **Custom guardrails** that various teams like risk management (model risk, tech risk, operational risk, etc.), technology, product, legal, cyber, and compliance can easily design and deploy with integrated monitoring of LLM usage.

3. Standardized and extensive **observability & reporting** that leverages explainable metrics.

In-house Apps Powered by GenAI

3rd Party Apps with Embedded GenAI

Foundation Model APIs

Call center assist

Legal assistant

Report summarizer

External chatbot

Internal search

salesforce

Adobe

zoom

AI Gateway

DynamoEval — Pre-production

DynamoGuard — Post-production

Initial Deployment Goal:

Establish trustworthy AI deployment at scale by stress testing and guardrailing 2 AI Applications
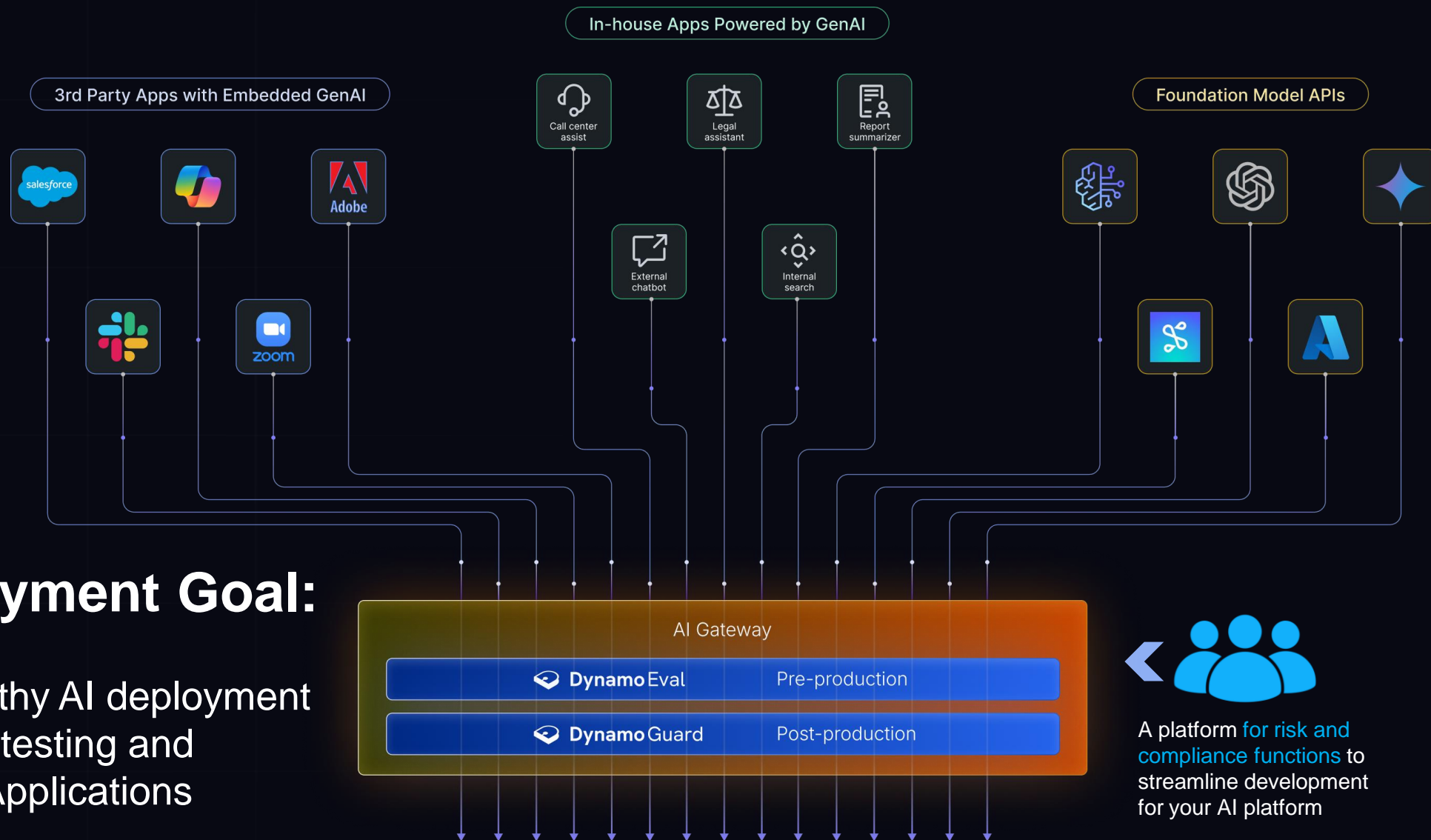
A platform for risk and compliance functions to streamline development for your AI platform

Proposed Delivery Operating Model

A comprehensive onboarding approach that integrates people, process, and technology will be required to drive success.

Executive Leadership

The deployment and ongoing relationship management will be overseen by Dynamo's Chief Product Officer and Co-Founder and Head of AI Compliance Strategy.

- Successful deployment will depend upon effective platform integration and line of defense use.
- Dynamo will host offsites and working sessions to promote effective use.

Dynamo Team Leads

Dynamo product and technical leads will manage day-to-day deployments to drive joint success. Core team will include:
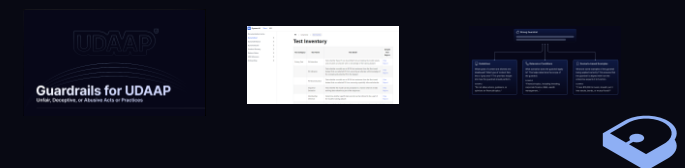
- Solutions Engineer / Project Management
- DynamoEval Product Specialist
- DynamoGuard Product Specialist
- Infrastructure and Integration Specialist

Weekly meetings and status reporting will facilitate on-time deployment

Adoption Acceleration

Dynamo's strategy focuses on accelerating adoption and ongoing engagement with key stakeholders

- Active and engaged user training sessions to facilitate onboarding
- In-depth product training guides
- Ongoing engagement through industry insights, guardrail recommendations, and community engagement for all lines of defense

Proposed Delivery Operating Model

Our cross-functional team of customer success, machine learning, and risk management experts provide ongoing support as you establish a comprehensive process to implement and operationalize Dynamo.

	Overview	Sample Deliverable
Customer Success Leads	Each customer gets a dedicated Customer Success Lead where a regular routine is setup for ongoing engagement and oversight. Through this relationship, Dynamo ensures our technology is fit for purpose, support requirements are addressed, and customers have access to Dynamo AI talent.	• Assigned customer success lead • Weekly Dynamo check-ins through engagement • Access to Dynamo team and GenAI events (deep-dive industry workshops)
Platform Technical Support	Dynamo establishes a hotline for engineering support, should inquiries arise. This is done via slack, email, or phone. Documentation suites are provided with initial delivery.	• Direct access hotline or slack channel • Ongoing Technical Support (with reporting) • Root cause analysis reports (if required)

Proposed Delivery Operating Model

Our cross-functional team of customer success, machine learning, and risk management experts provide ongoing support as you establish a comprehensive process to implement and operationalize Dynamo.

	Overview	Sample Deliverable
Machine Learning Guidance	Access to our machine learning team is given through the Customer Success Leads. Our team of highly trained Machine Learning experts is available to guide our clients with product inquiries.	• Access to industry-leading ML talent • Distributed ML recommendations and thought leadership material • Ad-hoc support with ML inquiries
AI Risk Management Advisory	Through a deep-dive AI operating model session, our AI Risk and Control Management expertise will engage your leadership team to ensure Dynamo AI is implemented effectively within your AI management lifecycle.	• Deep Dive Operating Model Framework Recommendations Document • Invitation to Dynamo AI client policy sessions (quarterly)
Training / Partner Reselling	Training is given through the initial implementation phase. A training plan is then established post deployment, either for the customer to initiate, or with Dynamo through periodic engagements for partner reselling opportunities.	• Dynamo Ongoing Training Recommendations • Established Dynamo AI-run training sessions (for partner / resellers)

Key Decisions & Dependencies

Key Client Decisions:

1. Identify stakeholders for guardrail training and SaaS access
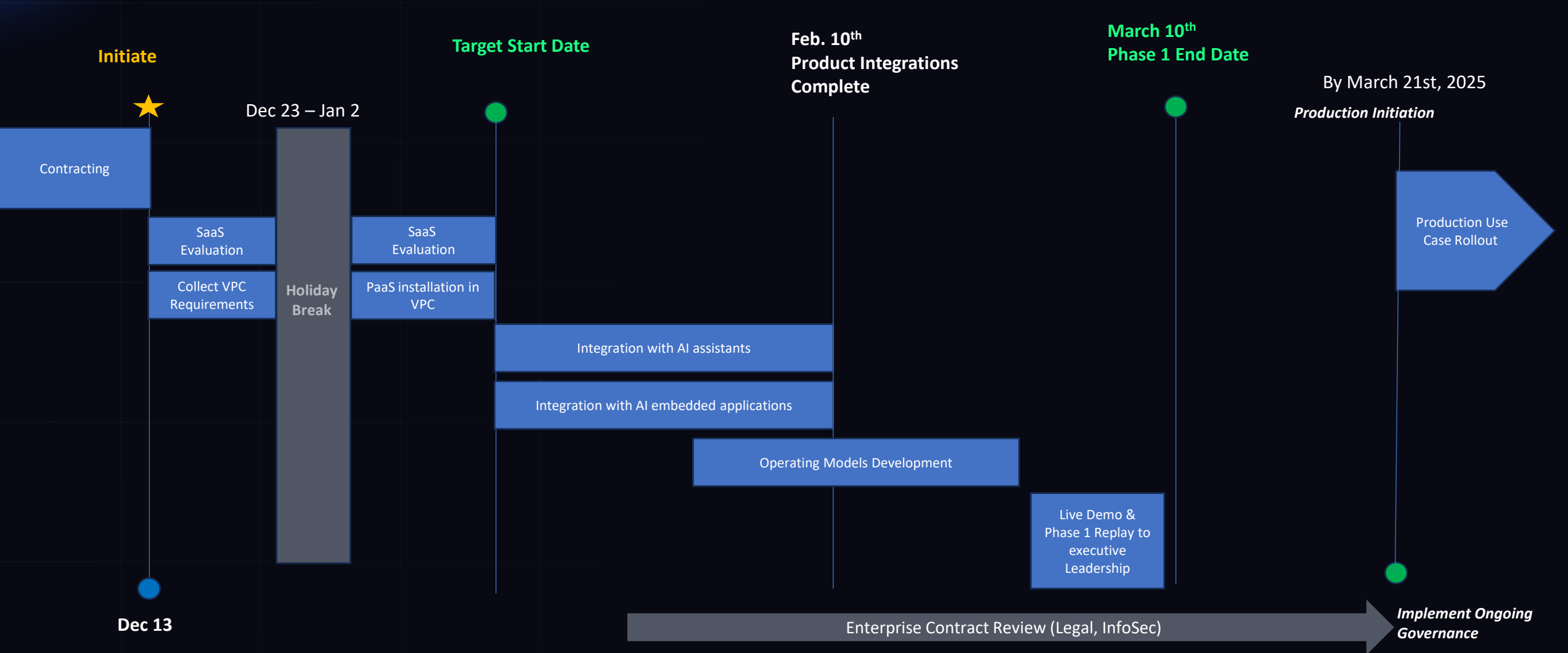2. Confirm timing of deployment kick off
3. Identify initial validation models or use cases for Dynamo platform integration
4. Finalize deployment environment details

Key launch dependencies:

1. Dedicated Point of Contact during deployment for Dynamo Team
2. Align existing platform timeline and requirements with Dynamo integration

Operating Model Deep Dive

Operating Model Guidance

Execute a Rapid 4-Week Effort to Develop GenAI Operating Model Framework Recommendations

Deliverables:

a) **Execute Guardrail Compliance Mapping Onsite Workshop:** Hold a 3-hour in person cross-functional stakeholder workshop to develop an inventory of customer-specific guardrails to deploy in Phase 2 that supports use cases, and considers its size, complexity, and regulatory considerations.

b) **Develop a tailored GenAI Operating Model Framework Recommendations Document that includes:**

- **Technical Controls Stakeholder Management Guidance:** Recommendations on which stakeholders should be responsible for proposing, creating, validating, deploying, monitoring, and reporting on technical controls.

- **High-Level Guardrail Development and Deployment Guidance:** Guidance on how to deploy effective guardrails, tailored to client specific organizational structure.

- **Redteaming Standards:** Standards for redteaming GenAI Use-Cases aligned to client specific operating models.

- **3rd Party Integration Recommendations:** Recommendations for integrating DynamoGuard with existing dashboarding, observability, security, identity, etc.

**Primary Point of Contact:**
Daniel Ross
Head of AI Compliance Strategy @ Dynamo

"*Dan Ross, Dynamo AI's Head of AI Compliance Strategy, has spent over 15 years advising financial institutions on regulatory and operational governance matters, most recently with Promontory Financial Group, and formerly as a technology strategy leader at Bank of America and Deutsche Bank*"

Operating Model Guidance

Our focus is to accelerate execution and effective oversight of AI risk management across all lines of defense

Line of Defense

1st

Line of Defense

2nd

Line of Defense

3rd

AI Controls Management and Oversight
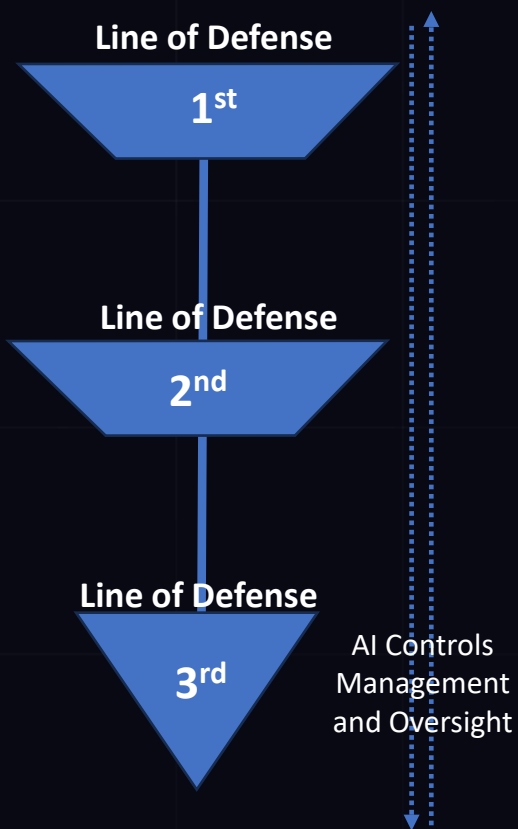
Empower the 1st LOD to implement AI controls with DynamoEval and DynamoGuard

- Apply comprehensive model evaluations and active guardrails in an easy-to-use and intuitive manner
- Reduce knowledge gaps and promote effective 2nd and 3rd LOD engagement with compliance reporting, standard taxonomies, and human-in-the-loop workflows
- Shorten time-to-market for AI use case implementation with customer and configurable AI controls

Deliver superior governance and oversight capability to the 2nd LOD

- Promote ownership of AI risk management standards with customized controls and human-in-the-loop workflows
- Map AI risk, ethics, and policy expectations to implemented evaluations and guardrails for effective oversight
- Utilize comprehensive control reporting and monitoring dashboards to facilitate effective oversight and testing

Inform Audit with comprehensive AI control insights from Dynamo AI

- Satisfy audit data requests with detailed and real-time risk metrics and reporting from Dynamo AI dashboards
- Facilitate risk-driven audit cycles with continuous access to real-time guardrail interactions
- Align on AI control terminology and KRIs with standard reporting across the 3LODs

Operating Model Guidance

Audit Deep Dive - Strengthen internal audit abilities with Dynamo insights

Comprehensive and automated GenAI risk evaluations allow audit deploy resource efficiently and effectively, incorporating risk-based targeted audits across the GenAI control lifecycle

Line of Defense

3rd

Strengthen audit GenAI skills and expertise
Cutting-edge evaluation results inform and upskill non-technical audit leaders and ensure focus is on the risks that matter

Implement risk-based targeted audits that match the evolving nature of GenAI
Real-time observability of model evaluations and guardrails (through a single-pane-of-glass view) facilitates a flexible audit schedule to respond to emerging risks and control failures

Assess effectiveness of guardrail control remediations in real-time
Reporting at audit's fingertips to assess the effectiveness of post-deployment guardrail remediation implementations

Informed by an independent evaluation layer of embedded GenAI vendors
Dynamo AI is an independent entity evaluating some of the largest GenAI providers, including vendor solutions with embedded AI

Operating Model Guidance

Operating Model for Gen AI Guardrails Creation, Evaluation, & Deployment

1. Guardrail policy definition and case study review

2. Train lightweight guardrail model

4. Calculate quantitative benchmarks

Policy Definition
- Legal
- Product
- Security

Initial Datapoint Review
- Legal (maybe)
- Product
- Security

Model Training

Quantitative Benchmark

Dynamo Generated Benchmark

Diverse Prompts	98%
Malicious "Jailbreaking"	92%
Borderline	92%
In Domain	94%

User Submitted Benchmark (optional)

Custom Benchmark	95%

For context, Meta claims >90% detection accuracy for content violations using its automated techniques.

https://transparency.meta.com/enforcement/detecting-violations/technology-detects-violations

- Product
- Security

Deployment into Production

Feedback

3. Customer tests guardrail in chatbot environment

Test Chatbot
- Legal (maybe)
- Product
- Security

The Platform for Compliant, Enterprise-Grade LLMs
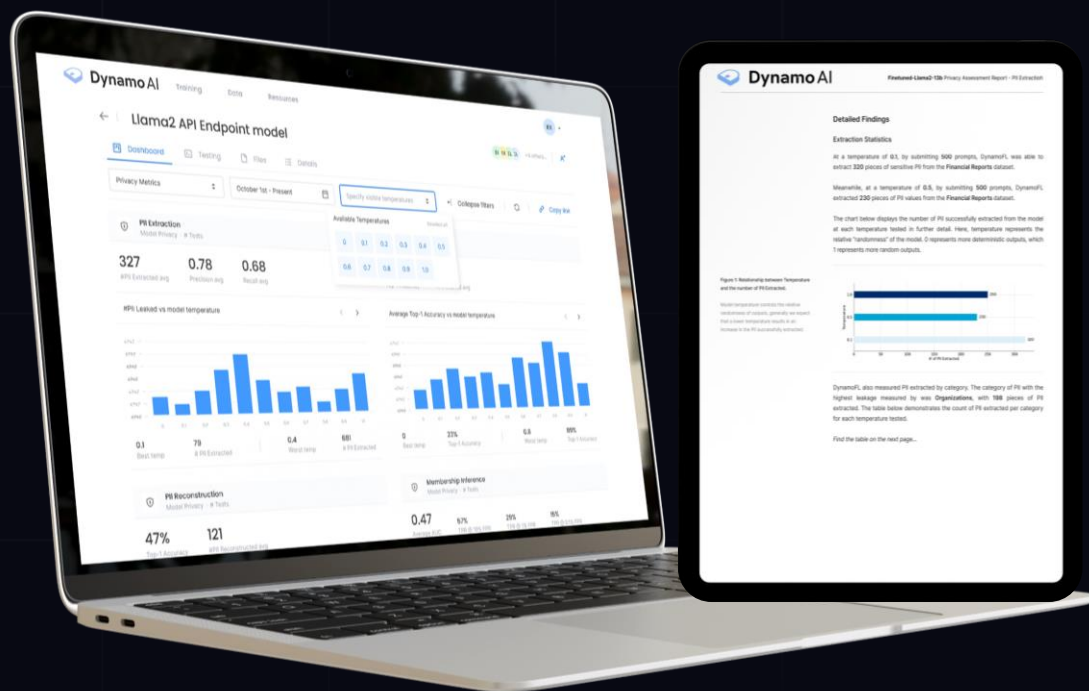
Integrated Privacy, Compliance Documentation, And Deployment

Integrations With Azure, AWS, GCP And Can Be Deployed Across Any Cloud Provider