DataRobot

SOLUTION BRIEF

AI Governance with DataRobot AI Production

Predictive models are an increasingly integral part of business processes across most industries. This creates a growing problem for properly integrating these models into the business process, as well as governing and monitoring these models at scale to ensure performance. As organizations advance in their adoption of predictive AI, add more tools to their technology ecosystem, and explore newer use cases, the number of models in production continues to increase exponentially, making model governance and monitoring even more complex. Often leaders are lacking visibility into which models are deployed, how they are impacting the business, and what risk they may pose. As enforcement of model regulations increases globally, there is an urgent need for enterprise-scale model governance and compliance documentation.

A robust AI governance framework helps to mitigate these challenges associated with AI in production without hindering its value to the business. DataRobot AI Production provides a centralized control and command center giving you the seamless ability to test, document, deploy, monitor, and govern a diverse portfolio of models in production no matter where they're built or deployed. Going beyond standard MLOps capabilities, it provides a system of record for all your AI assets. This helps you establish a framework to maintain governance and audit trails for all AI deployments across your entire organization with automated versioning, compliance documentation, and even tracking custom business metrics. With DataRobot AI Production, you don't have to wonder if your models pose a potential risk, and you will be prepared to handle any audit or inquiry from regulators.

After the financial crisis of 2008, regulators around the world began to monitor model risk management practices in earnest, starting with the U.S. Federal Reserve Board (FRB)'s SR 11-7. This issue is now trending globally with the EU AI Act[1] released in 2021, and CP6[2] from the Bank of England in June 2022. Regulatory attention and the need for responsible practices to curb model risk in financial markets has only grown with the rapid increase in adoption of machine learning.

The sheer volume of models that financial service institutions are deploying has skyrocketed to optimize performance, taxing teams' operational capacity. A lack of production framework in the AI lifecycle creates clogged pipelines and leaves already overstretched teams with an overwhelming amount of work around maintenance and explainability.

Volume isn't the only concern. Over the last several years, models have gotten increasingly complex with modeling techniques and algorithmic advancements moving beyond traditional linear regression models. And what happens when one model depends on another? More varied datasets that include both structured and unstructured data add to the challenge.

The volume of models and complexity compounds the concern for managing these models and the risks posed and further amplifies the need for proper governance and model risk management. Meanwhile, regulators are quickly catching up and not only enforcing existing regulations, but increasing them to ensure responsible AI governance frameworks, particularly in financial services.

1800% Growth
in the number of bills passed that contain "artificial intelligence" across 25 countries between 2016 and 2021[3]

25% Jump
in the number of models for U.S. banks since 2019[4]

[1]ArtificialIntelligenceAct.eu, [2]Bank of England, Model risk management principles for banks, [3]Stanford, Measuring trends in artificial intelligence, [4]McKinsey & Company, Model risk management 2.0 evolves to address continued uncertainty of risk-related events

Chief risk officers and business leaders need to balance an enormous variety of factors to manage model risk responsibly.

Do they spend more to keep up with model demand or accept higher risk? How do they tackle a shortage of qualified talent for performing model validations? Is it feasible to manage multiple models across different lines of business without a centralized inventory?

The consequences of a poorly developed AI governance framework include job loss, brand or reputational damage, financial setbacks, reduced operating performance, or punishing fines.

Finally, businesses can't ignore the danger of being outpaced by competitors if they fail to keep up with trends in AI modeling.

U.S. $97 million:
An SEC settlement imposed on four Transamerica entities in 2017 for misleading customers[5]

50% of Banks
in a 2021 survey already considered AI or ML capabilities part of their definition of a model.[6]

How well is your business managing model risk?

When you're considering your ML governance framework, ask yourself these questions:

- **How many models can you successfully support?**
- **Can you easily trace model origin, versions, and deployment history?**
- **Do you know who created your models, with what data, when, and for which use case?**
- **Do you have a central way to track model performance metrics such as drift, accuracy, and custom business KPIs?**
- **How do you uncover and remediate issues?**
- **What's the resource cost for your AI governance framework?**

[5]U.S. Securities and Exchange Commission, Transamerica Entities to Pay $97 Million to Investors Relating to Errors in Quantitative Investment Models
[6]KPMG, Modern strategies for a bold new era of Model Risk Management

What does an effective AI governance framework look like?

AI governance establishes the rules and controls for your machine learning models, including access, testing, validation, logs, and tracking results. With a proper governance framework in place, teams move faster, use AI more often, and manage risk more actively. All of this means that you can scale your machine learning investment and be sure you're aligned with regulatory requirements.

Clear roles and responsibilities ensure that your team members know where they fit into workflows.

Establish clear roles like production model manager or validator within your model lifecycle. Each role description should include duties, qualifications, capabilities, and any training or certification requirements.

Access control helps teams maintain control over production environments.

You should limit access to production data for model training, deployment, modification, or A/B testing, either at the individual user level or through role-based access control (RBAC).

Change and audit logs ensure legal and regulatory compliance.

Knowing when a change occurred and who made it is critical for compliance, as well as troubleshooting when something goes wrong. The system should record actions from both people and software applications or agents.

Records of action support troubleshooting and follow-ups.

For each change to production data, models, or systems, users should provide notes on why they took action that other team members or auditors might find useful. These records can also be beneficial for troubleshooting.

Production testing and validation ensure quality.

To maintain quality, you need to test and validate each new or refreshed model before deployment. Logging these tests and their results demonstrates that models are approved and ready for production.

DataRobot

The model history and version library record model versions as they evolve.

Models will change over time as you update and replace them in production. Maintaining a complete model history, including model artifacts and changelogs, is critical for legal and regulatory compliance.

Traceable model results ensure you meet legal and regulatory obligations.

Building reports for your model results and their deployment status supports both business goals and internal operations. At the same time, it's essential to understand where bias arises in your modeling process.

Data versioning and version tracking provide insights into the lineage of your models.

As your training and production data change over time, a deployed model loses its predictive power. That's known as "data drift." Establish rules around how much data drift is acceptable for your organization's purposes.

Model documentation tracks and presents your results.

Compliance documentation provides evidence that your models work properly, they're appropriate for their intended business purposes, and they're conceptually sound.

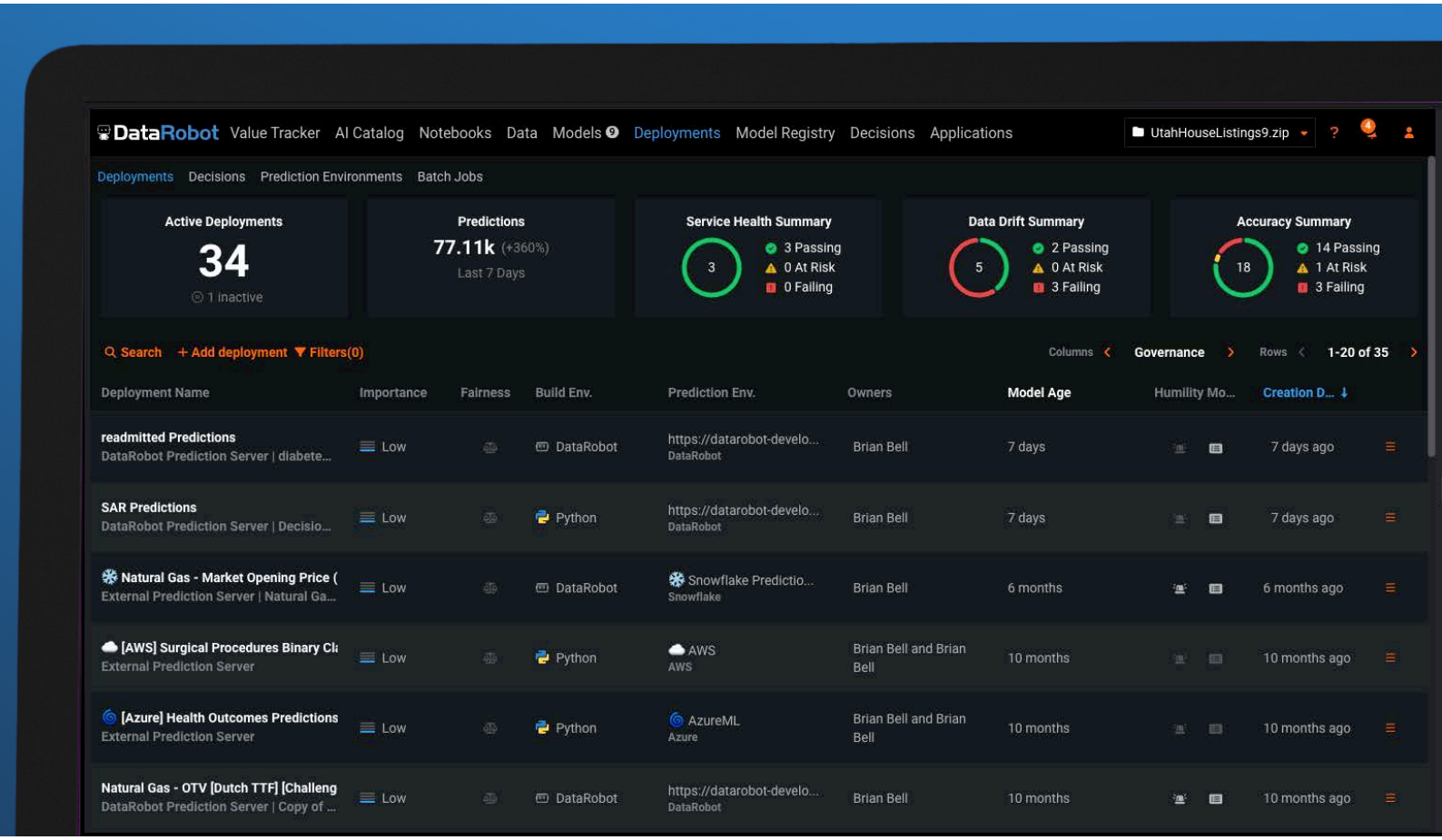
A model inventory houses and manages your models and metadata.

A well-organized and highly navigable model inventory means your people can organize, manage, and access models easily. It supports streamlined assessment, candidate management, continuous evaluation, retraining, and A/B testing.

DataRobot

DataRobot AI Production provides a proven AI governance framework

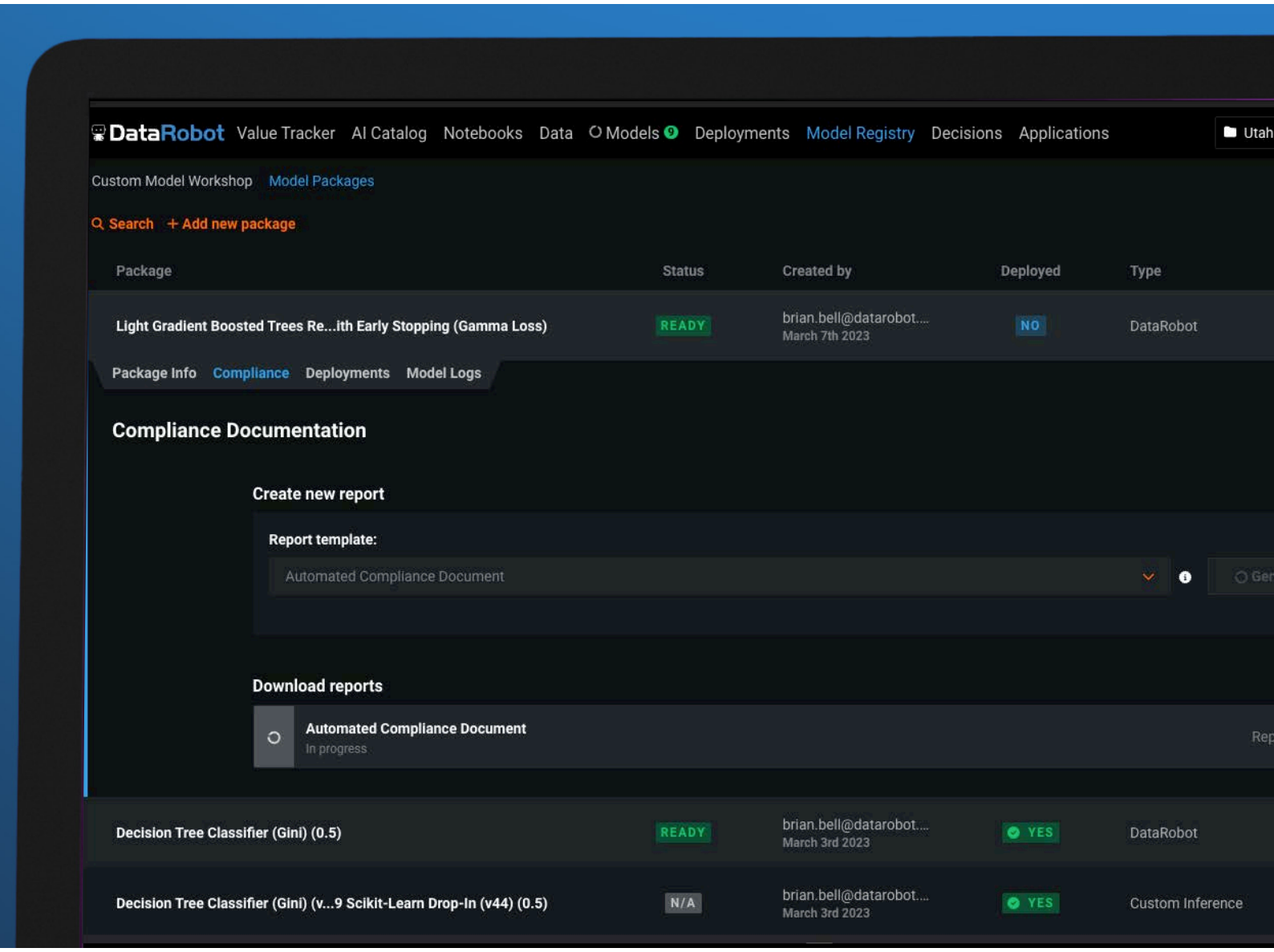
With DataRobot AI Production, ML engineering and data science teams can integrate models into any DevOps process, deploy to any production environment, and easily govern and monitor all deployments from one central command center. As a result, your teams have the confidence to deploy AI models in a well-governed, secure, and compliant environment, accelerating their path to business value. Empower your data scientists to focus on innovation while your ML engineering and IT teams benefit from easy integrations, automated compliance, and streamlined production.



One place for MLOps management and performance monitoring

A single system of record for all of your AI artifacts helps to manage all production models no matter who built them, how they were built, or where they are hosted. You can drill down into detailed performance analysis of each deployment such as exploring drift of text features or tracking custom business KPIs associated with a model.

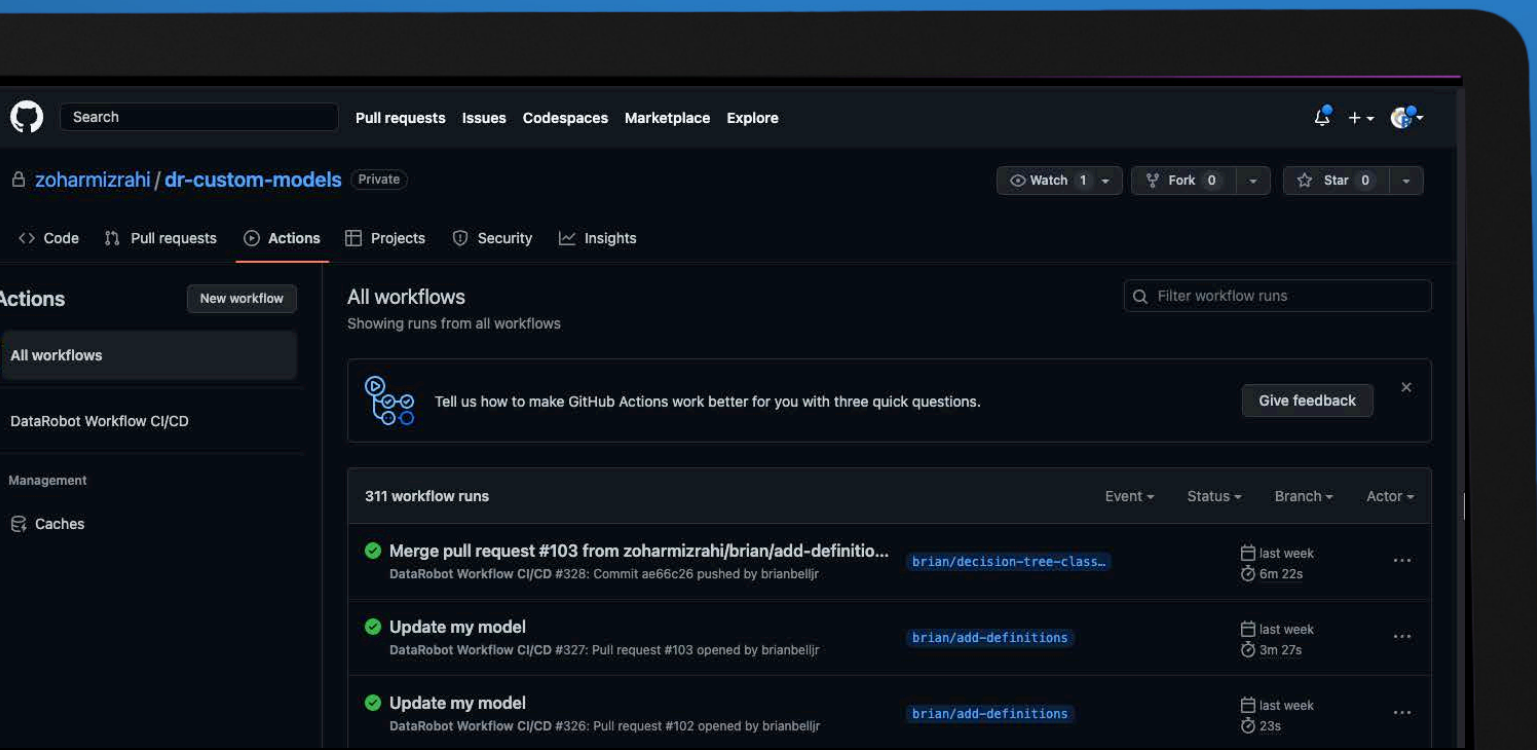
DataRobot AI Production unifies your infrastructure by providing centralized roles, governance, and object structure to minimize risk and manage your entire model inventory. You can easily set up role-based approval workflows, access controls, and manage change when personnel turn over.



One-click compliance documentation for any model

Automated model compliance documentation saves your data science team hours of manual work and decreases the time-to-deployment for models. The documentation provides evidence that the components of the model work as intended, that the model is appropriate for its intended business purpose, and that it is conceptually sound. With a single click you can generate model documentation for any model, regardless of where a model was built or where it is deployed.

Model compliance documentation can be customized to accommodate enterprise or industry-specific requirements. You can bring in your own custom datasets, charts, tables, and URLs to enrich and standardize model documentation across your organization.



Integration with DevOps and CI/CD processes

DataRobot AI Production gives you the interoperability you need across your ecosystem. You can easily integrate your models across tools you already use, such as Airflow for data orchestration or GitHub Actions for CI/CD. This ensures that you can seamlessly manage and govern all your AI pipelines across all environments.

You can maximize your investments in data platforms, DevOps tools, and chosen cloud AI models in alignment with your chosen IT governance, environment, and business rules. With broad interoperability and automation, AI governance is simpler and less resource-intensive for your teams.

DataRobot is the leader in Value-Driven AI – a unique and collaborative approach to AI that combines our open AI Platform, deep AI expertise and broad use-case implementation to improve how customers run, grow and optimize their business.

DataRobot AI Production is more than just MLOps. The platform enables organizations to deploy, manage, monitor, and govern their machine learning models from a single place, empowering different stakeholders to seamlessly collaborate around the common goal of scaling and managing trusted AI models in production.

Our proven combination of cutting-edge software and world-class AI implementation, training, and support services, empowers any financial services organization to drive better business outcomes with AI.

Learn more about DataRobot AI Production
datarobot.com/platform/#production

Sign up for a demo
datarobot.com/demo

DataRobot

Contact Us

225 Franklin Street, 13th Floor, Boston, MA 02110, USA

datarobot.com info@datarobot.com