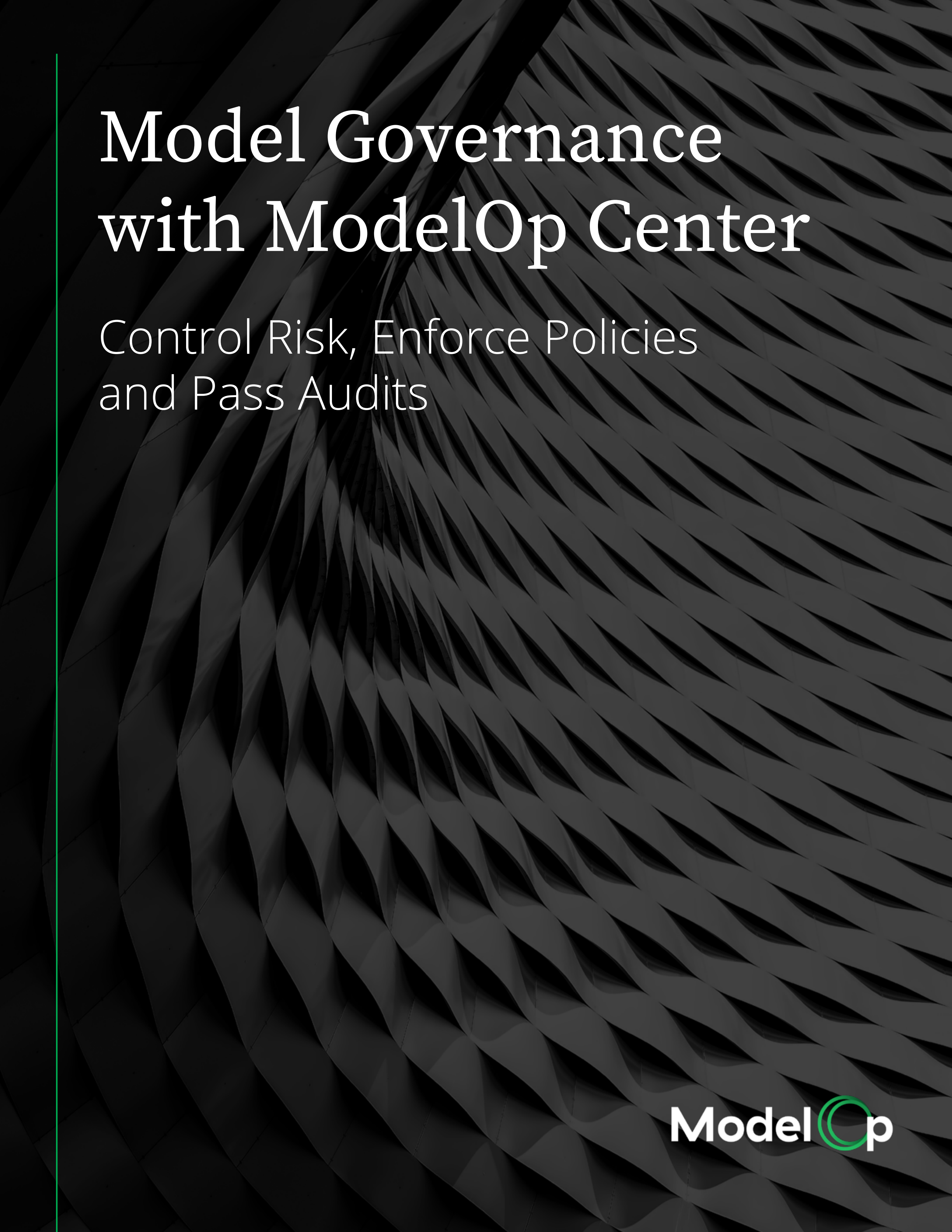
Model Governance with ModelOp Center

Control Risk, Enforce Policies and Pass Audits



ModelOp

Table of **Contents**

Increased AI Model Usage Doesn’t Have to Result in Increased Risk

Across your enterprise, the use of AI models continues to expand. As AI is deployed across more teams, the business benefits can continue to proliferate. However, without the right governance capabilities, this expanded AI usage can also present the business with massive risk.

As AI models expand across teams and technologies—and regulatory requirements continue to grow more stringent—manual, ad hoc governance efforts simply don’t cut it.

That’s why you need ModelOp Center.

With ModelOp Center, your team can establish unified, automated governance over AI models deployed across the organization. With the solution, your teams can dramatically streamline model governance, while you ensure continuous compliance with internal policies and external regulations.

AI Models: Increasing Criticality, Scope and Complexity

Within enterprises, reliance on AI has continued to grow. In the process, everything associated with AI is also expanding:

Increasing Criticality

AI models are playing an increasingly foundational role in business-critical decision making and processes, and addressing more strategic applications. In the process, these models continue to play a more prominent role in the ultimate fortunes of the business.

Expanding Scope

These models are being implemented by more and more teams, who are deploying expanding numbers of models. Over time, the scale of implementations, including data volumes, numbers of users and integrations also continues to climb.

Mounting Complexity

Along the way, complexity also continues to proliferate, with different models, development platforms, deployment environments and so on all continuing to expand. Increasingly, model development and validation are being conducted both onshore and offshore, which can further complicate matters.

Intensifying Regulatory Scrutiny

Models are often subject to regulatory oversight. The rules teams have to comply with continue to evolve, while the scrutiny only increases. In the financial services sector, the Federal Trade Commission (FTC) enforces a number of laws that apply to the use of models, including the Fair Credit Reporting Act and the Equal Credit Opportunity act. More generally, organizations need to ensure AI models and other data management practices comply with such privacy regulations as the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Further, more regulations are expected. For example, the Office of the Comptroller of the Currency (OCC) and several other agencies are investigating the use of AI models, which is expected to yield updated rules for financial firms. Also, in April 2021, the European Commission released draft regulation on AI, which is anticipated to form the basis of a comprehensive EU law on automated decision making.

For all these reasons, the governance of AI models grows both more critical, and more difficult.

> *“Sharpening the organization’s thinking about show-stopping risks is only a start. Also crucial is the application of company-wide controls to guide the development and use of AI systems, ensure proper oversight, and put into place strong policies, procedures, worker training, and contingency plans.”*
>
> **McKinsey Global Institute**

The Governance Challenges

For IT and risk management leaders, the growth of AI presents some mounting responsibilities.

The development and use of AI models have to be governed to ensure compliance with internal policies and relevant regulatory mandates. Ultimately, the models in place can prove to be a major asset, or a major vulnerability, and having the right governance in place can make all the difference.

The problem many teams are facing is the fact that so many deployments have sprung up in an isolated fashion. Across many organizations, a number of different teams are now running AI models. Invariably, each team has its own processes, tools and platforms.

This siloed, fragmented approach presents several key challenges:

- **Lacking central production model inventory.** When confronted with basic questions—such as "how many models are running in production?"—risk management, IT and other teams lack clear answers. Assets and artifacts, such as data sets used to train models, approval histories, source code files and so on, are in varying repositories and formats, and difficult to find and track.

- **Lacking consistent processes.** Because models are developed and deployed in a disparate fashion, there's no consistent process in place. Further, because many teams that are now deploying AI models don't have risk management backgrounds, they may lack formal processes, and may skip important approvals and gating workflows.

- **Lacking consistent, comprehensive monitoring.** Because models are developed and deployed in a disparate fashion, there's no consistent process in place. Further, because many teams that are now deploying AI models don't have risk management backgrounds, they may lack formal processes, and may skip important approvals and gating workflows.

The Implications

Right now, the status quo is creating a range of issues and obstacles in organizations:

- **Manual, time-consuming efforts.** Given the lack of centralized tracking and asset aggregation, teams are constantly resorting to manual, time-consuming efforts needed to assess status, run reports and so on.

- **Reactive.** Too often, central IT and risk teams are not finding out about models until after they're deployed. Rather than being able to proactively manage compliance, risk teams are being forced to respond after an audit has been initiated or a policy breach has been discovered.

- **Lack of consistency in policies and policy enforcement.** Across teams, there aren't formal definitions of requirements and processes. Due to this inconsistency, it is difficult to ensure each model goes through the required gates, approvals and checkpoints.

- **Lack of visibility.** Given the lack of centralized, unified model governance, it is either time consuming or downright impossible to accurately assess models. For example, if an internal auditor wants to validate the data used to train a given model, it may be extremely difficult to find the actual version of the data set used.

- **Lack of scale.** Within many organizations currently, governance happens manually. Various teams are generating reports and aggregating data from various spreadsheets. When one or two models are running, this kind of ad hoc, piecemeal approach to governance may suffice, but it fundamentally can't scale beyond that. This is particularly true given the complex, heterogeneous nature of model deployments running across the enterprise, and the intensifying, evolving nature of regulatory oversight.

- **Exposure.** With only sporadic, ad hoc monitoring, enterprises are constantly exposed to the risk of models running in a non-compliant fashion. Ultimately, the details matter, but more importantly, the ability to ensure policies and processes are adhered to—and that those controls can be demonstrated, is critical.

The end result? Particularly in financial services, organizations are exposed to excessive risk. In many cases, the result has been that organizations have been hit with penalties of tens and even hundreds of millions of dollars—all due to a lack of consistent policy enforcement and compliance breaches. In fact, two of the 10 largest regulatory fines issued in 2020 were related to insufficient risk management controls, and accounted for fines of $400 million and $85 million.

Scenario: How Do Audits Play Out in Your Organization?

An auditor asks you for a complete list of models running across the organization.

How do you gather and report on the information? Sending emails to various teams and then gathering and consolidating spreadsheets? Or do you hit a button and generate a report?

Next, the auditor wants details about a specific model, including who it was approved by, what data was used to train the model, when it was put into production and so on. Does this precipitate another labor-intensive, search/aggregate/report effort? Or is all this information also readily available?

Requirements

While tools are available that offer basic tracking of workflows, those capabilities don't address the critical need for comprehensive model governance. To establish effective, authoritative and efficient governance, teams need to address these requirements:

- **Standard, documented definitions.** First, it is essential to create standardized definitions of key concepts, most fundamentally, starting with what a model actually is. Teams must also be able to categorize what constitutes a high, medium and low risk model; and then establish a lifecycle aligned with that categorization. In this way, for example, teams can consistently ensure that high-risk models are given the highest levels of scrutiny.

- **Complete model inventory.** In a central fashion, teams need to be able to gain visibility of all models, across teams, tools, domains and technologies. For consistent, efficient compliance with internal policies and external regulations, comprehensive sets of assets need to be tracked and captured. Ultimately, teams need detailed traceability of all specifics around each model running, including source code samples and details around approvals and approvers.

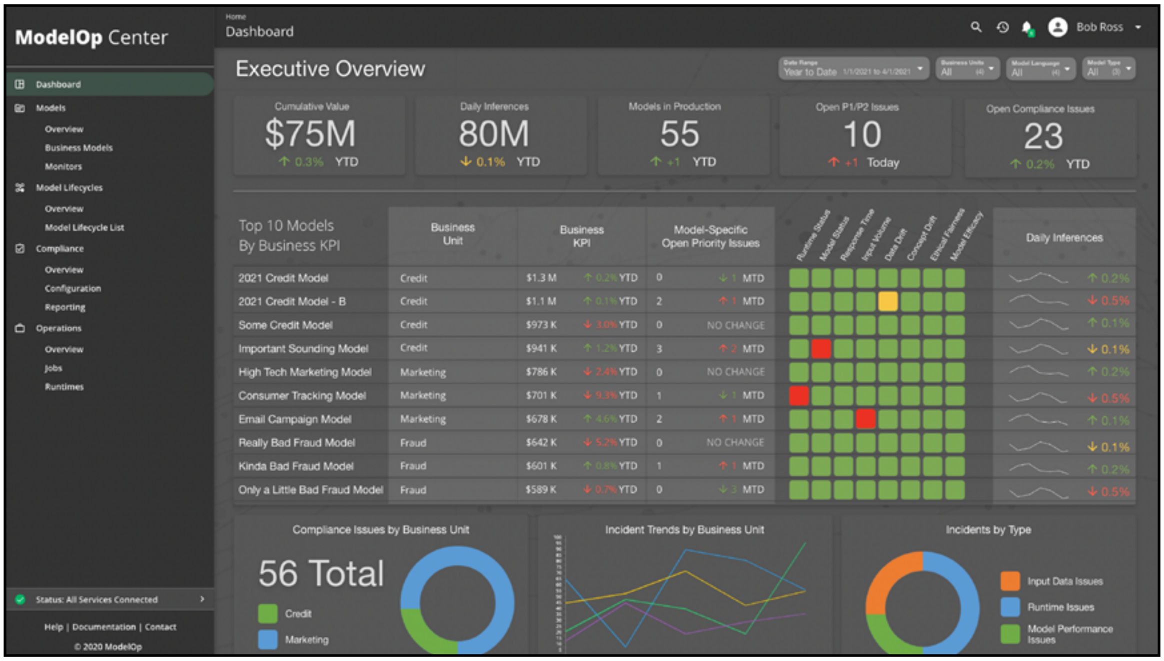
- **Comprehensive monitoring.** Teams need to establish consistent, comprehensive monitoring of models. This includes monitoring for performance as well as data, ethics and fairness. In this effort, it is important to be able to establish custom, intelligent thresholds in order to ensure that teams are only getting alarms when real issues arise, rather than getting a bunch of false alerts. In addition, it is important to ensure risk management and IT governance teams are given the opportunity to review and approve these thresholds.

The Solution: ModelOp Center

ModelOp Center offers enterprises a way to centrally, consistently and efficiently manage all their AI and ML models. The solution enables teams to optimize the entire model operations lifecycle, from initial deployment through to retirement. With ModelOp Center, teams can automate and orchestrate comprehensive governance workflows.

With the solution, you can:

- Use a rules-based engine to automate monitoring and enforcement of controls.
- Leverage governance controls to ensure model quality and compliance.
- Gain complete flexibility to align your implementation with your organization's specific technologies, policies and objectives.
- Get started with customizable processes that speed initial set up.
- Achieve fast, efficient and authoritative auditing and compliance reporting.



Executive Overview

Cumulative Value: $75M ↑ 0.3% YTD

Daily Inferences: 80M ↓ 0.1% YTD

Models in Production: 55 ↑ +1 YTD

Open P1/P2 Issues: 10 ↑ +1 Today

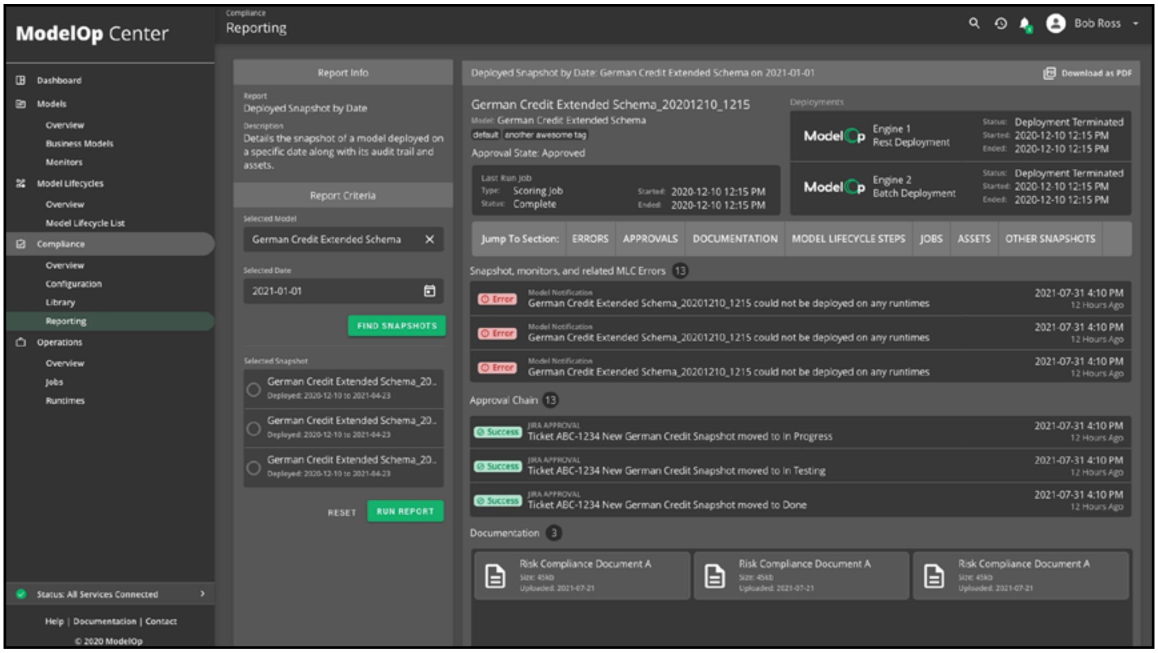
Open Compliance Issues: 23 ↑ 0.2% YTD

Top 10 Models By Business KPI	Business Unit	Business KPI		Model-Specific Open Priority Issues		Runtime Status	Model Status	Response Time	Input Volume	Data Drift	Concept Drift	Ethical Fairness	Model Efficacy	Daily Inferences
2021 Credit Model	Credit	$1.3 M	↑ 0.2% YTD	0	↓ 1 MTD	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↑ 0.2%
2021 Credit Model - B	Credit	$1.1 M	↑ 0.1% YTD	2	↑ 1 MTD	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	↓ 0.5%
Some Credit Model	Credit	$973 K	↓ 3.0% YTD	0	NO CHANGE	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↑ 0.1%
Important Sounding Model	Credit	$941 K	↑ 1.2% YTD	3	↑ 2 MTD	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	↓ 0.1%
High Tech Marketing Model	Marketing	$786 K	↓ 2.4% YTD	0	NO CHANGE	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↑ 0.2%
Consumer Tracking Model	Marketing	$701 K	↓ 9.3% YTD	1	↓ 1 MTD	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↓ 0.5%
Email Campaign Model	Marketing	$678 K	↑ 4.6% YTD	2	↑ 1 MTD	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	↑ 0.1%
Really Bad Fraud Model	Fraud	$642 K	↓ 5.2% YTD	0	NO CHANGE	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↓ 0.1%
Kinda Bad Fraud Model	Fraud	$601 K	↑ 0.8% YTD	1	↑ 1 MTD	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↑ 0.2%
Only a Little Bad Fraud Model	Fraud	$589 K	↓ 0.7% YTD	0	↓ 3 MTD	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	↓ 0.5%

Complete Capabilities for Defining Governance Processes

ModelOp Center facilitates fast, efficient and complete establishment of governance processes that are tightly aligned with your organization. The solution aids in the definition of formal descriptions of processes, standards, categories and requirements. Through the solution, you can define how often a model needs to be monitored in production, specify revalidation and retirement dates and so on.

Further, through the solution's flexible integrations and APIs, ModelOp Center can seamlessly leverage data, metadata and files submitted elsewhere and also integrate with additional systems and workflows, such as creating a change request in Jira or service ticket in ServiceNow. With the solution, you can define a model in the lifecycle editor of choice, and then easily onboard it into ModelOp Center. (See the page below for complete details on all the solution's **integration capabilities**.)



Report: Deployed Snapshot by Date

Description: Details the snapshot of a model deployed on a specific date along with its audit trail and assets.

Selected Model: German Credit Extended Schema

Selected Date: 2021-01-01

Selected Snapshot:

- ○ German Credit Extended Schema_20..
Deployed: 2020-12-10 to 2021-04-23
- ○ German Credit Extended Schema_20..
Deployed: 2020-12-10 to 2021-04-23
- ○ German Credit Extended Schema_20..
Deployed: 2020-12-10 to 2021-04-23

Deployed Snapshot by Date: German Credit Extended Schema on 2021-01-01

German Credit Extended Schema_20201210_1215

Model: German Credit Extended Schema

default | another awesome tag

Approval State: Approved

Last Run Job
Type: Scoring Job
Status: Complete
Started: 2020-12-10 12:15 PM
Ended: 2020-12-10 12:15 PM

Deployments

ModelOp	Engine 1 Rest Deployment	Status: Deployment Terminated Started: 2020-12-10 12:15 PM Ended: 2020-12-10 12:15 PM
ModelOp	Engine 2 Batch Deployment	Status: Deployment Terminated Started: 2020-12-10 12:15 PM Ended: 2020-12-10 12:15 PM

Snapshot, monitors, and related MLC Errors 13

Error	Model Notification German Credit Extended Schema_20201210_1215 could not be deployed on any runtimes	2021-07-31 4:10 PM 12 Hours Ago
Error	Model Notification German Credit Extended Schema_20201210_1215 could not be deployed on any runtimes	2021-07-31 4:10 PM 12 Hours Ago
Error	Model Notification German Credit Extended Schema_20201210_1215 could not be deployed on any runtimes	2021-07-31 4:10 PM 12 Hours Ago

Approval Chain 13

Success	JIRA APPROVAL Ticket ABC-1234 New German Credit Snapshot moved to In Progress	2021-07-31 4:10 PM 12 Hours Ago
Success	JIRA APPROVAL Ticket ABC-1234 New German Credit Snapshot moved to In Testing	2021-07-31 4:10 PM 12 Hours Ago
Success	JIRA APPROVAL Ticket ABC-1234 New German Credit Snapshot moved to Done	2021-07-31 4:10 PM 12 Hours Ago

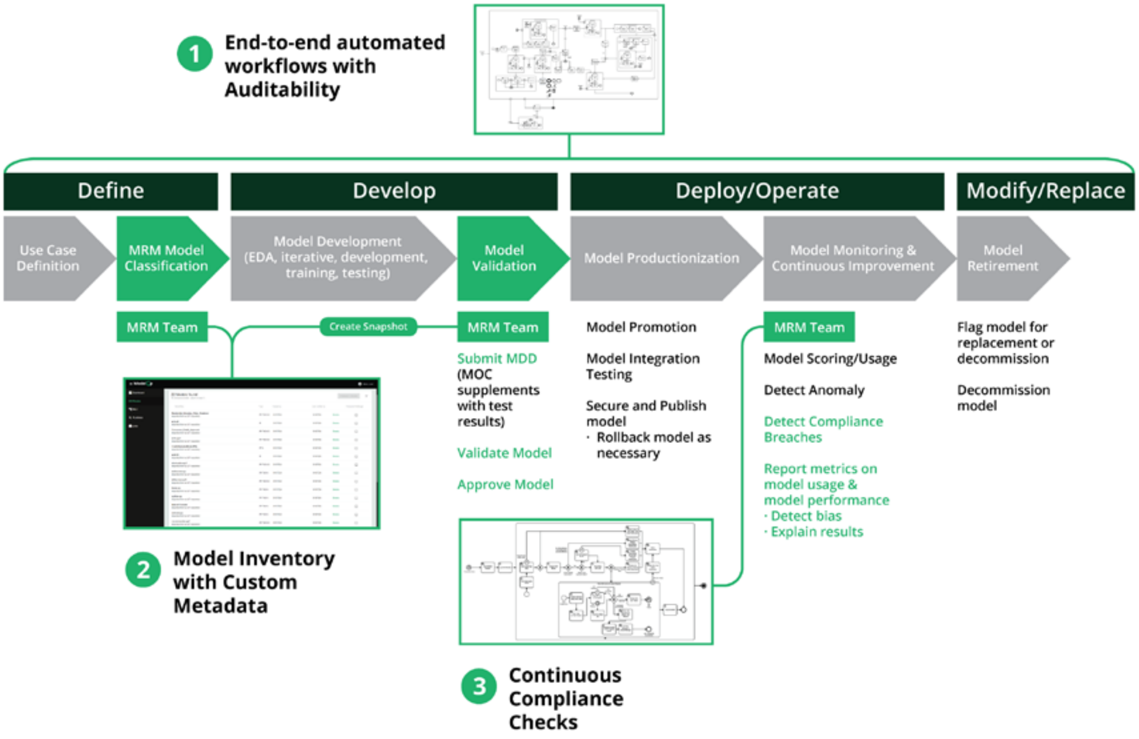
Documentation 3

Risk Compliance Document A Size: 45kb Uploaded: 2021-07-21	Risk Compliance Document A Size: 45kb Uploaded: 2021-07-21	Risk Compliance Document A Size: 45kb Uploaded: 2021-07-21

Orchestration and Automation

ModelOp Center provides complete support for the entire model operational lifecycle, including model approval, validation, deployment, change, compliance and controls and retirement. Through the solution, a single command, such as "register model" can trigger all required approval workflows.

Leveraging orchestration and automation, risk management and IT governance teams can much more efficiently and consistently enforce controls across different organizations. With the solution, your teams can orchestrate simple workflows, for example, triggering an alert if a model's expiration date is reached. You can also support more complex decision tables, enabling your teams to define intricate model risk management rules. For example, in the case above, a notification can not only be automatically generated once an expiration date has been reached, but, if the model continues operating for a specified threshold, such as several days, without any updates or resolution, if approved, the solution can automatically decommission the model and update its status accordingly.

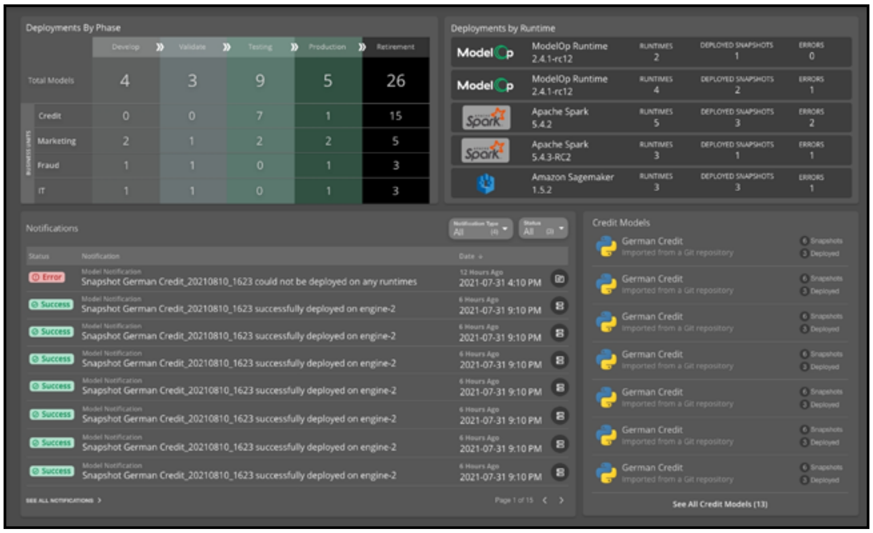

1 End-to-end automated workflows with Auditability
Define
Develop
Deploy/Operate
Modify/Replace
Use Case Definition
MRM Model Classification
Model Development (EDA, iterative, development, training, testing)
Model Validation
Model Productionization
Model Monitoring & Continuous Improvement
Model Retirement
MRM Team
Create Snapshot
MRM Team
Submit MDD
(MOC supplements with test results)
Validate Model
Approve Model
Model Promotion
Model Integration Testing
Secure and Publish model
· Rollback model as necessary
MRM Team
Model Scoring/Usage
Detect Anomaly
Detect Compliance Breaches
Report metrics on model usage & model performance
· Detect bias
· Explain results
Flag model for replacement or decommission
Decommission model
2 Model Inventory with Custom Metadata
3 Continuous Compliance Checks

Continuously Updated, Authoritative Model Inventory

With ModelOp Center, you can track each step in the model's lifecycle, so you can gain full transparency and auditability. With the solution, you can maintain a comprehensive production model inventory that includes required documentation and assets, such as:

- Model ID
- Model documentation, including design documents
- Snapshots of every version and model source
- Code
- Reviewers and approvers, including specific steps in review, such as whether a model was rejected, approved, or approved with conditions
- History of all jobs executed
- Test metrics
- Training data

Through this comprehensive production model inventory, ModelOp Center helps you establish complete, immutable snapshots of models. As a result, even years after deployment, if issues or audits arise, you can still produce details on how the model was developed, who approved it, the training data used and so on. You can even provide auditors with complete reproducibility of model functionality at a given point in the model lifecycle.



Deployments By Phase

	Develop	Validate	Testing	Production	Retirement
Total Models	4	3	9	5	26
Credit	0	0	7	1	15
Marketing	2	1	2	2	5
Fraud	1	1	0	1	3
IT	1	1	0	1	3

Deployments by Runtime

	RUNTIMES	DEPLOYED SNAPSHOTS	ERRORS
ModelOp Runtime 2.4.1-rc12	2	1	0
ModelOp Runtime 2.4.1-rc12	4	2	1
Apache Spark 5.4.2	5	3	2
Apache Spark 5.4.3-RC2	3	1	1
Amazon Sagemaker 1.5.2	3	3	1

Notifications

Notification Type: All (4) Status: All (3)

Status	Notification	Date ↓
Error	Model Notification Snapshot German Credit_20210810_1623 could not be deployed on any runtimes	12 Hours Ago 2021-07-31 4:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM
Success	Model Notification Snapshot German Credit_20210810_1623 successfully deployed on engine-2	6 Hours Ago 2021-07-31 9:10 PM

SEE ALL NOTIFICATIONS › Page 1 of 15 ‹ ›

Credit Models

German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed
German Credit Imported from a Git repository	6 Snapshots 3 Deployed

See All Credit Models (13)

Monitoring: Establish Continuous Compliance Verification

With ModelOp Center, establishing monitoring of new models is extremely fast and efficient, so you can ensure ongoing enforcement of regulatory, business and risk control policies. The solution offers these advanced capabilities:

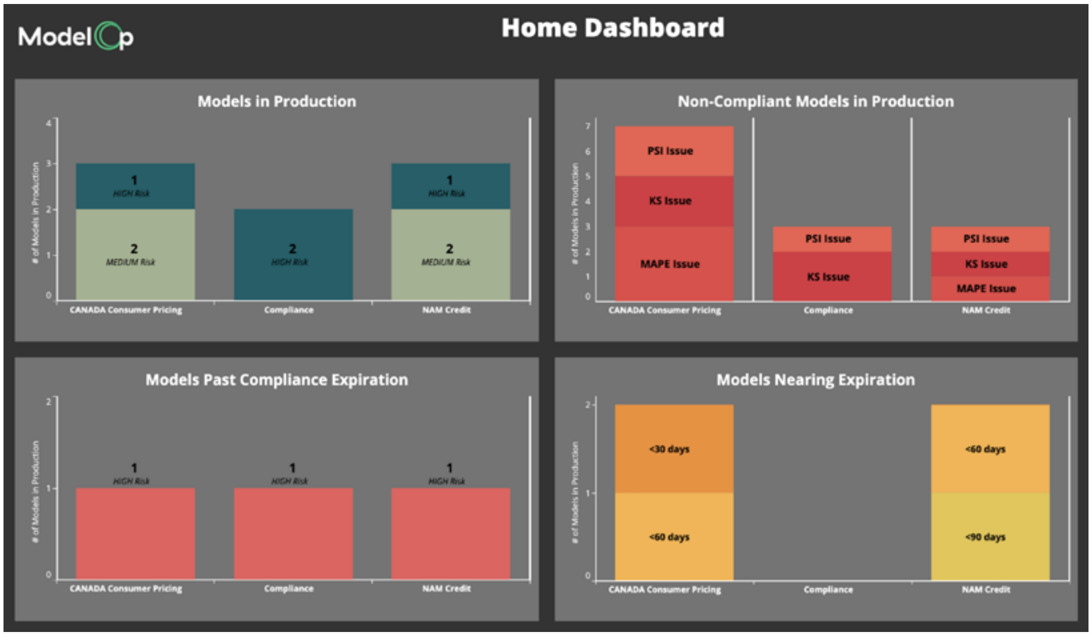
- **Fast, efficient implementation.** The solution features pre-built models that can be used immediately and customized as needed for your specific requirements.

- **Comprehensive coverage.** ModelOp Center can monitor statistical, technical and infrastructure performance issues. The solution offers monitors that cover a range of areas, including data drift, concept drift, ethical fairness, interpretability, population scoring, characteristic stability, champion/challenger testing, Shap testing and more.

- **Advanced orchestration and automation.** With its advanced capabilities, ModelOp Center enables your teams to automate a range of activities, including detecting issues with operational performance, enforcing risk and governance controls and orchestrating problem remediation and updates. For example, the solution offers integration with ServiceNow and other IT service management platforms for incident and change management.

- **Granular threshold configuration.** ModelOp Center offers intelligent benchmark and threshold setting capabilities, so you can minimize false positives and negatives. It also can help ensure IT and risk management teams approve thresholds before implementation.

With these capabilities, the solution enables your teams to foster continuous compliance and model improvement.



Seamless, Flexible Integration and Model Support

With its advanced capabilities and flexible integration, ModelOp Center provides one platform for managing all your AI, ML and analytics models.

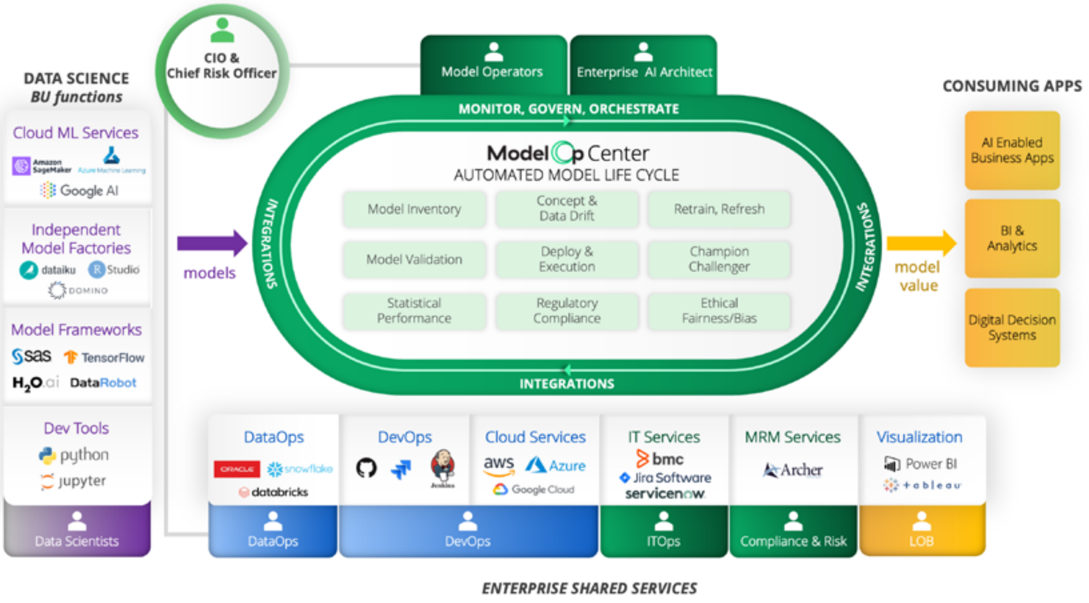
With the solution, you can manage models built with a wide range of development tools and frameworks, whether you have teams working with R, Python, C, Scala or all of the above. You can also centrally track models running on premises and in a broad range of cloud environments.

ModelOp Center seamlessly integrates with your enterprise ecosystem, including your model development tools, IT systems, risk management systems and business applications. The solution features more than 40 pre-packaged integrations. Further, the solution’s RESTful API makes it easy to add support for new technologies and applications whenever needed.

ModelOp Center Features More Than 40 Prepackaged Integrations

- AI model factories
- Model frameworks
- Model workbenches
- Shared IT systems
- Cloud-based ML services
- BI visualization tools

View the Full List of **ModelOp Center Integrations**.



Enabling Governance for Risk, IT and Data Teams

ModelOp Center represents one platform that can support all aspects of model governance, delivering the capabilities each of these different teams require:

- **Risk management.** Through integration with model risk management systems, your teams can ensure compliance thresholds are adhered to at all times.

- **IT governance.** The solution supports governance throughout the IT lifecycle. With the solution, you can define and manage workflows through development, quality assurance, user acceptance testing, integration testing and SecOps testing to ensure there are no vulnerabilities. If issues are detected, teams can seamlessly, automatically open change requests in ServiceNow, run modifications by IT governance change review boards, route for SecOps review and so on—with all progress updates tracked in the model inventory.

- **Data governance.** For teams dedicated to ensuring that models operate in an ethical, unbiased fashion, ModelOp Center offers extensive capabilities. With the solution, teams can quickly access the data used to train models and evaluate whether bias was introduced, private data was used in a non-compliant fashion and so on.

The Benefits of ModelOp Center

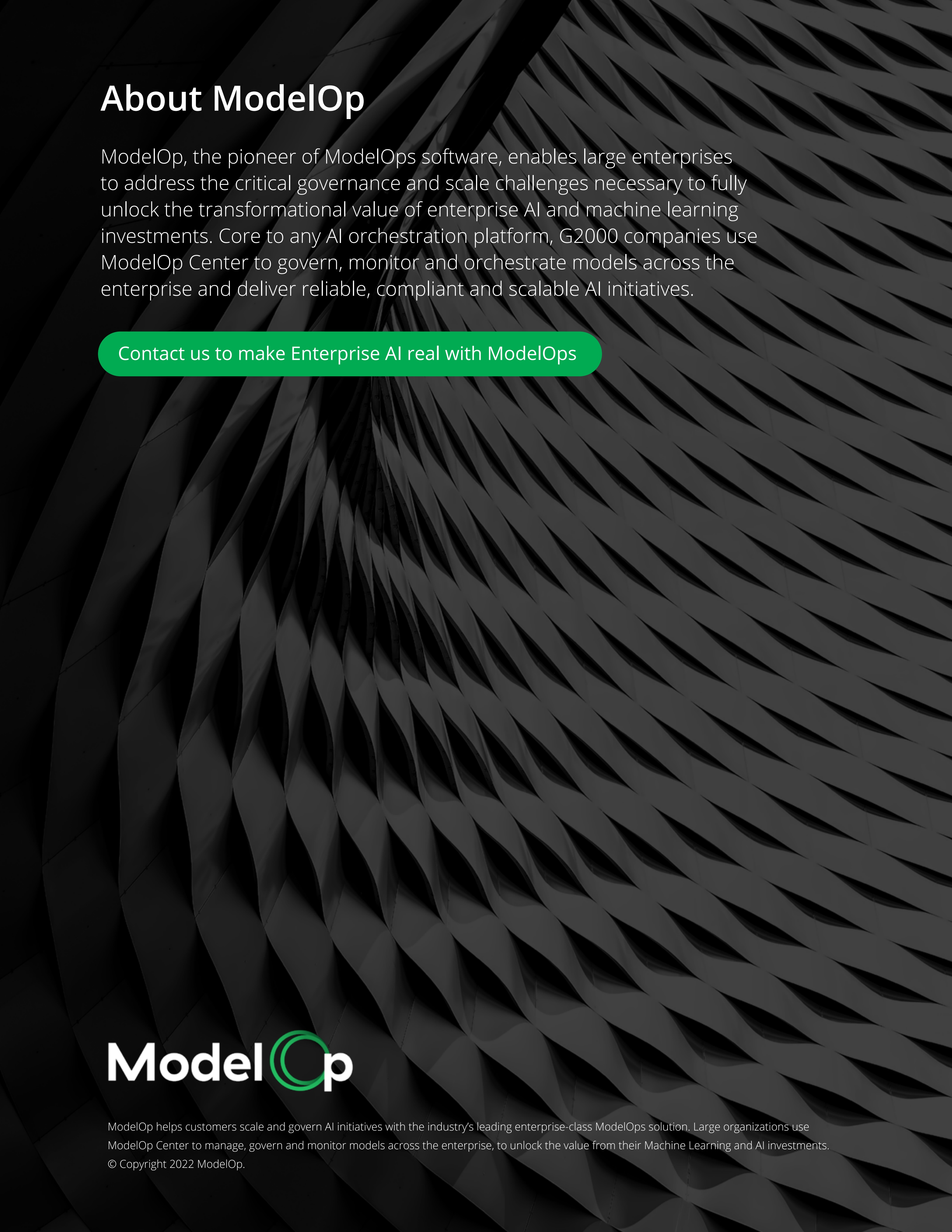
By implementing ModelOp Center, your team can realize these key advantages:

- **Streamline governance.** ModelOp Center delivers the central, powerful and unified controls and visibility that can significantly boost staff efficiency and productivity. With the solution, your teams can eliminate wasted time and inefficiency associated with emailing requests, aggregating spreadsheets, chasing down artifacts from disparate sources and so on. Through the solution's automation, teams can reduce overall workload associated with model validation and governance by 20-30%.

- **Boost compliance.** ModelOp Center enables the automation, process standardization and unified control and visibility that help promote more consistent policy compliance across the organization. The solution offers all the capabilities teams need to establish standardized, repeatable, demonstrable and auditable governance processes. With these capabilities, your teams can significantly reduce the business risk associated with poorly performing, faulty, biased or non-compliant AI models.

Conclusion

With manual, ad hoc governance, your teams simply can't scale to support your diverse AI models and technologies, increasingly large-scale and business critical applications and evolving regulations and internal policies. That's why you need ModelOp Center. With the solution, you can establish the automation, unified visibility and control and continuous monitoring that dramatically streamline governance and boost compliance.



About ModelOp

ModelOp, the pioneer of ModelOps software, enables large enterprises to address the critical governance and scale challenges necessary to fully unlock the transformational value of enterprise AI and machine learning investments. Core to any AI orchestration platform, G2000 companies use ModelOp Center to govern, monitor and orchestrate models across the enterprise and deliver reliable, compliant and scalable AI initiatives.

Contact us to make Enterprise AI real with ModelOps

ModelOp helps customers scale and govern AI initiatives with the industry's leading enterprise-class ModelOps solution. Large organizations use ModelOp Center to manage, govern and monitor models across the enterprise, to unlock the value from their Machine Learning and AI investments.