ALGORITHMIA

Q&A from Algorithmia's webinar featuring Forrester
Eight must-haves for MLOps success and when to use them

Answers from

Mike Gualtieri

Vice President and Principal
Analyst at Forrester Research

FORRESTER®

Q: Typically any new initiative (no matter what it is) fails 70% of the time. Any idea why the failure rate is twice as much in ML?

A: The main challenge is operationalizing ML—which is where machine learning operations (MLOps) comes in. Since ML is new and many people in organizations don't understand it, it might not go through that working backwards process like software development might. As a company gets more successful and has more people involved, the discipline that exists in software will start to get applied more to data science and machine learning teams. Just because you want a model to predict something in the end doesn't mean that it necessarily will. I think that really contributes to the high failure rate.

Q: Why should my organization adopt MLOps?

A: Any organization that wishes to implement machine learning must adopt MLOps to operationalize models for business value. Without MLOps, the process takes too long and is fraught with technical and business challenges, just with one model. What about a dozen use cases and models? A hundred? A thousand? To handle that, enterprises need MLOps—a rapid, repeatable, and scalable process that AI teams can use to implement more high-ROI AI use cases and manage them continuously across the AI model lifecycle.

Q: When I adopt MLOps, what problems will it solve for my organization?

A: Forrester's definition of MLOps is "tools, technology, and practices that enable cross-functional AI teams to efficiently deploy, monitor, retrain, and govern AI models in production systems". The key word in this definition is "efficiently". The AI lifecycle must be continuous if it is to be successful. Data engineers acquire and prepare data. Data science and machine learning teams analyze that data to create models. Developers integrate those models into applications. Infrastructure operations pros provision and manage the infrastructure needed to run applications and models. The process cycles on as teams retrain models from new data to redeploy them. All of these hand-offs are fraught with messiness and mistakes. MLOps brings automation and discipline at any scale.

> It's common for even a single ML use case to result in millions of dollars of business value.
>
> —Mike Gualtieri, Forrester Research

Q: What are the types of ML security vulnerabilities that I need to be aware of as I take models into production?

A: Model integrity and data protection are paramount. The model that is deployed must be the model intended to be deployed. That means that the lineage of the model must be tracked from training to deployment. Deploying the wrong version of the model or a maliciously modified version of the model can have dire business consequences. Likewise, the data, if sensitive, used during scoring or inferencing must be authorized, authenticated, and logged for future auditing.

Q: What does governance of ML models look like throughout the entire ML lifecycle?

A: To be governed, ML models must have versioning, lifecycle lineage, and security capabilities—so that any team member can access what others have done, replicate it, validate it, and build on it. This means: Track metadata, lineage, provenance, data, orchestrate workflows, and security compliance.

Q: How should I introduce MLOps into my organization?

A: It's common for even a single ML use case to result in millions of dollars of business value. The more use cases, the more value. MLOps is an essential capability to confidently and efficiently scale ML use cases. Data science teams and broader AI teams should compare their current operationalization process to MLOps capabilities presented in the webinar. Identify the gaps and then look for solutions in the market that will quickly fill those gaps. An investment in an MLOps solution will likely pay off with just a single use case and certainly as an organization scales to multiple models and multiple use cases.

Watch the full webinar →