# How to Avoid Breeding Bad Agents

Data Integrity ensures Accurate AI for Managed Risks

Tricentis
Data Integrity

# Curtis O’Dell

*Global Director Data Integrity*
*Tricentis*

## A bit about me

- Passionate leader in Tech for data's business value realization, with proven successes. IT Business leader with over 120m in ARR built over career. IPO and M&A veteran.
- I also have a proven track record of creating and delivering value from data analytics with AI, such as identifying fraud and opportunities, generating revenue, and reducing costs. I built my own version of probability for the data work I created and own the IP.

**Curtis O'Dell**

Global Business Manager @ Tricentis | Driving Global Busi...

# **IT Executives** response to AI

The hype train has left the station

**67%**

**Integrate Gen AI**

of enterprises will integrate gen AI into their AI strategy

**79%**

**ERP cloud migration**

of executives are using generative AI in app modernization projects

**65%**

**Build custom apps**

will integrate Gen AI in building, managing and delivering new apps

**$6.6T**

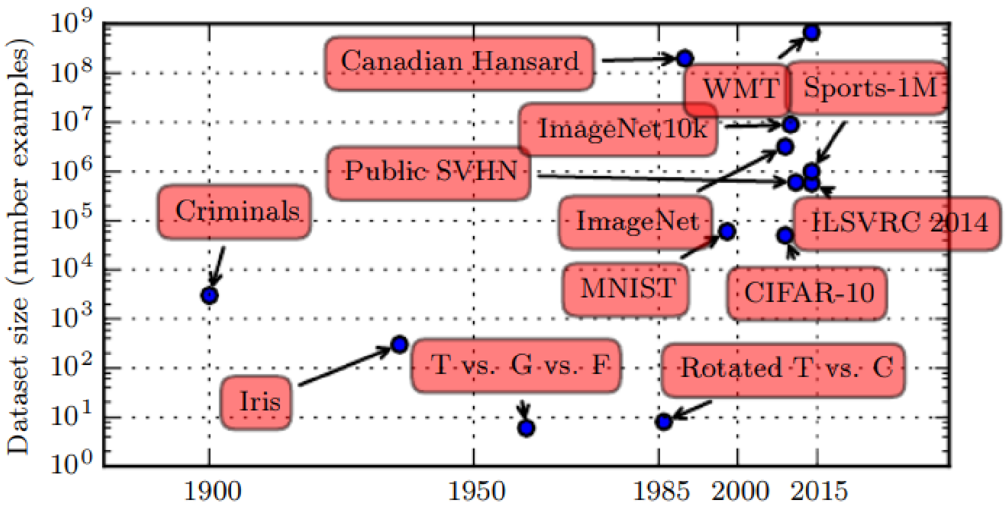
**Improve productivity**

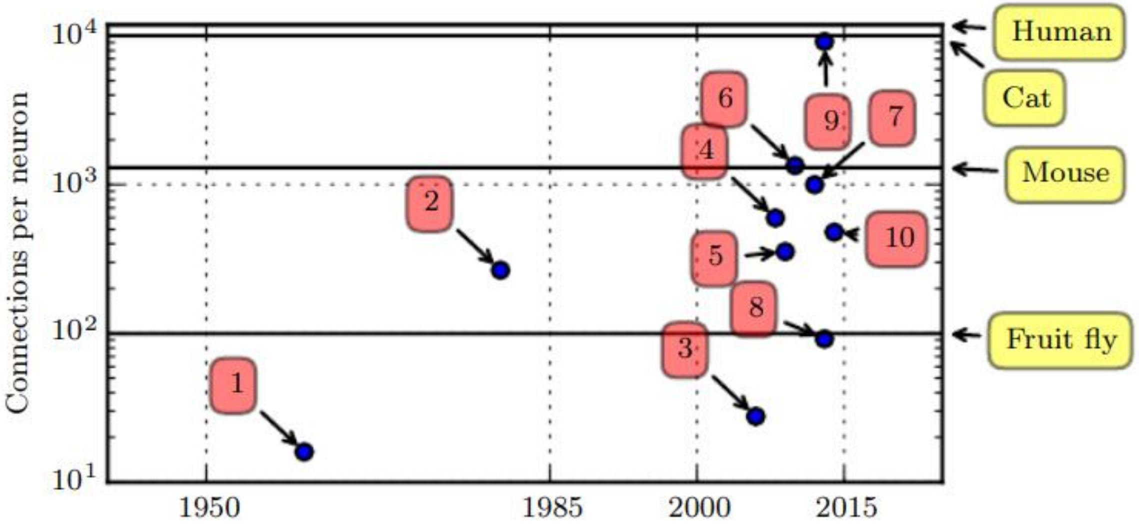
USD contributed by 2030 from increased productivity, 80% of total benefit*

* PwC's Global Artificial Intelligence Study | PwC

# AI / ML Why Now?

- Datasets move up in size to astronomical levels Data Explosion for training data catalyst #1
- Neuron connections has exponential levels

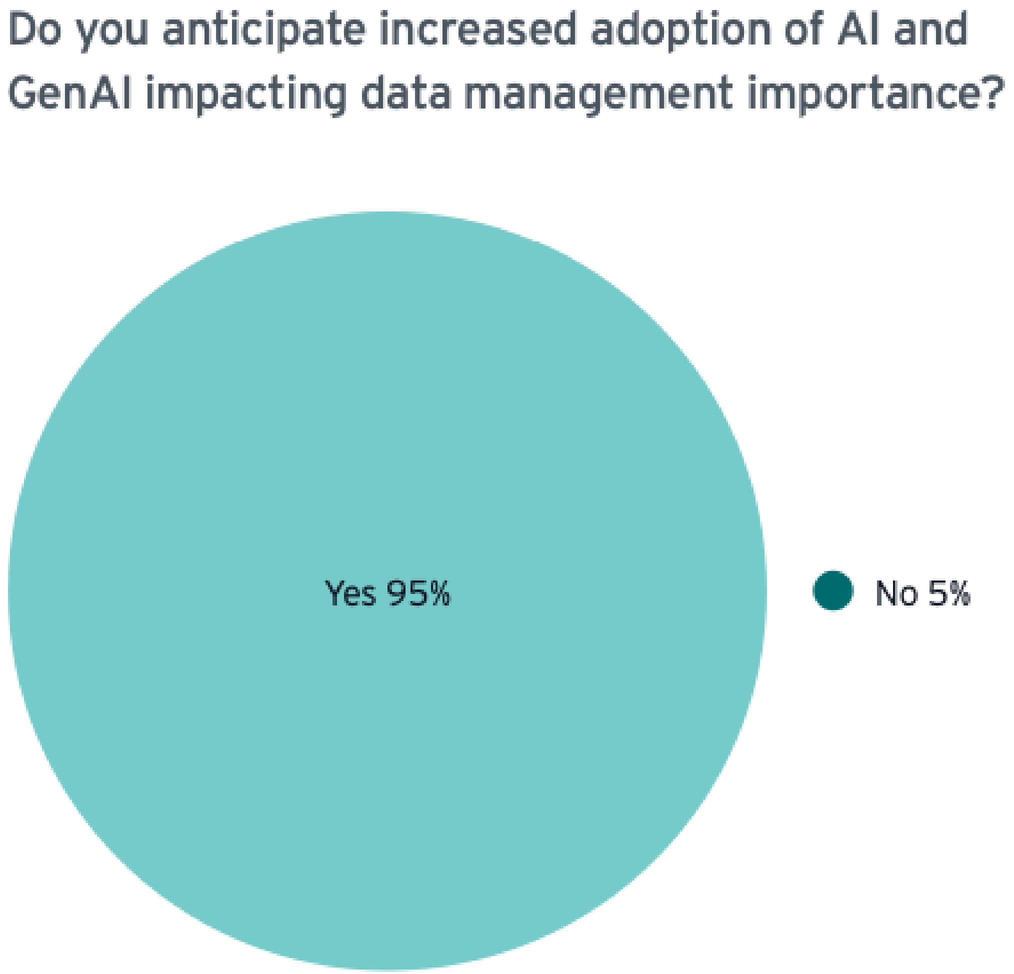




Deep Learning
by Aaron Courville, Yoshua Bengio, Ian Goodfellow

# AI Readiness and Data Quality

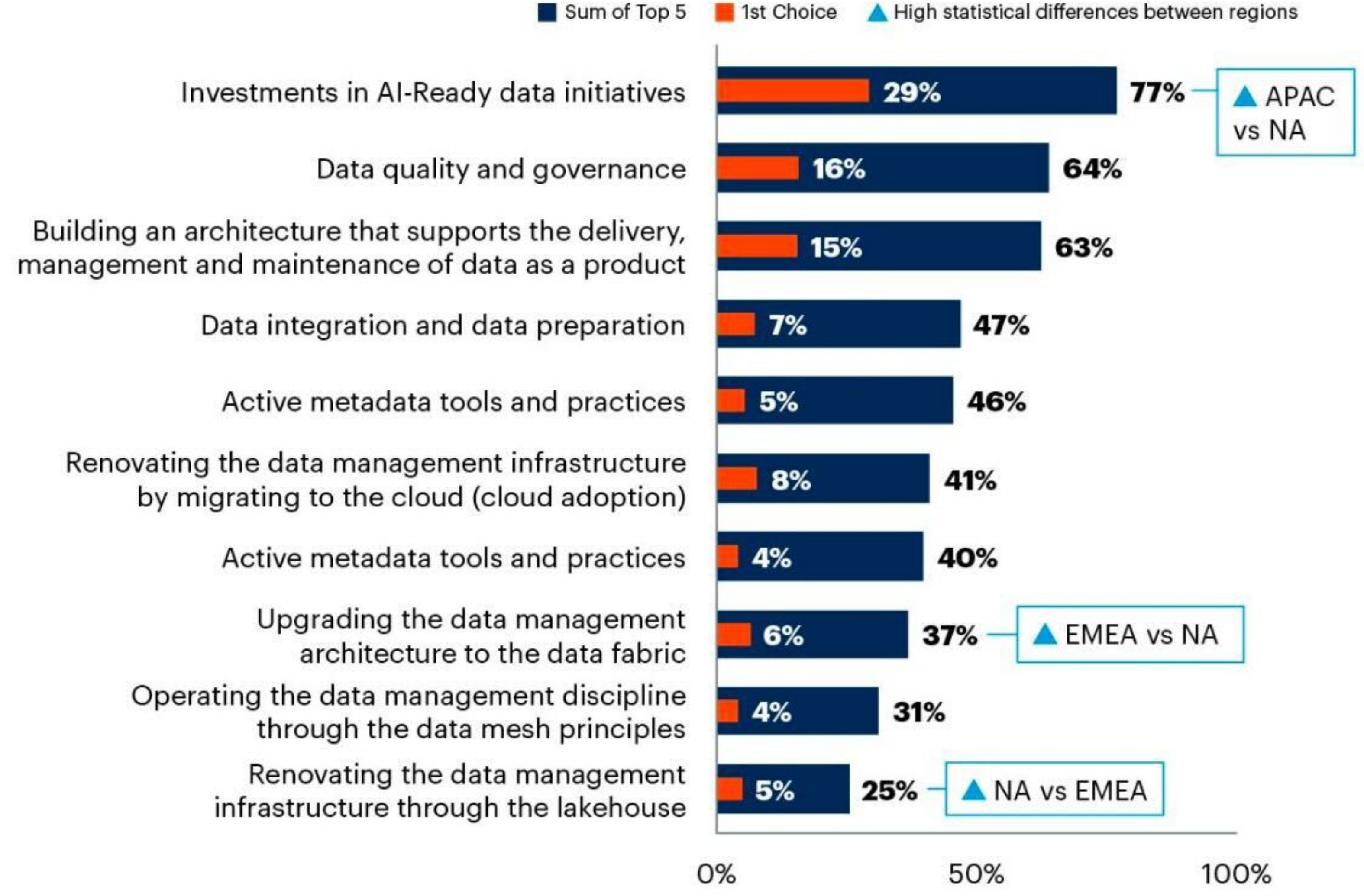
- 7 Key Points to Consider when thinking about AI Ready Data
  - AI-ready data strategy
  - Knowledge management
  - Data governance
  - Master data management
  - Data risk and compliance
  - Data quality
  - AI-ready data architecture



*NASCIO report: Your AI Blueprint: 12 Key Considerations as States Develop Their Artificial Intelligence Roadmaps*

# #2 AI Data Management Investment by CIOs

Top 5 Investment Trends in the Next 2-3 Years



n = 247; All Respondents excluding Not Sure

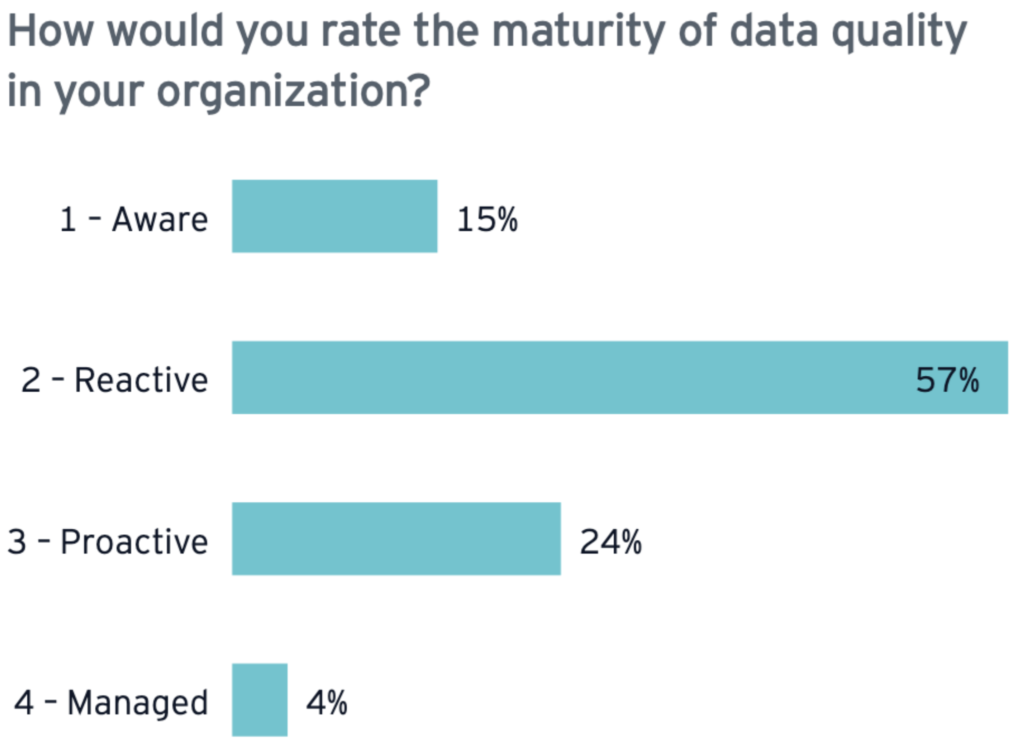
Q10: What do you think are the top 5 investment trends for data management leaders in the next 2-3 years?

Source: 2024 The Evolution of Data Management Survey

821077_C

# Data Quality Needs Data Governance

- Data errors can negatively impact mission delivery, constituent trust, and increase costs
- Without a data governance program in place, your organization runs the risk of utilizing poor quality data across the organization leading to fines, poor constituent experience, and failed initiatives.



*Data quality – vital to optimizing GenAI: A Survey of state chief information officers and chief data officers*

# Massive Data, Massive Models, Massive potential

## Model Sizes

**Classical Intelligence:**

80bn Neurons

**2020 AI:**

1.5bn Neurons

**2024 AI:**

1.35T Neurons

## Dataset Sizes

**Standard 2010's:**

15k data

**2020's Fraud:**

2 million records

**2024 AI:**

15 Trillion tokens

**185m ChatGPT users**

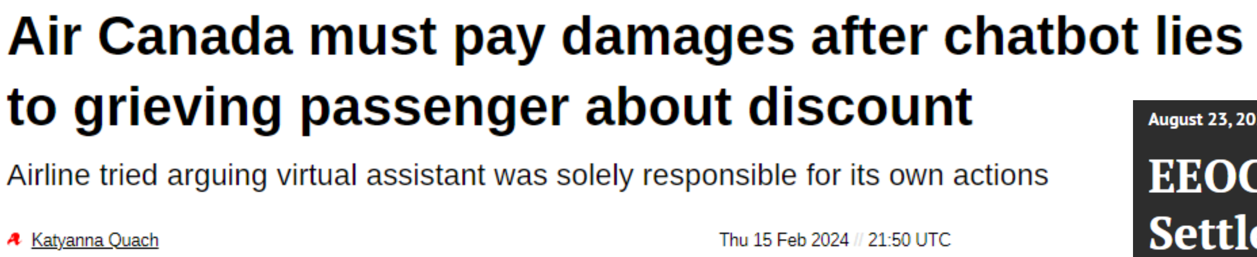
# Data Management Practices – is your data ready?

- Good Data Management looks like....
  - Addressing potential risk early and often
  - Effectively preparing for AI/ML journeys
  - Establishing Robust data practices

- But are you there yet?
  - Can your data keep up?
  - Can you trust accuracy of your data and thus your AI?
  - Is your data compliant?

DATA ENGINEERS WHEN ASKED..
'OUR DATA QUALITY IS READY FOR AI?'

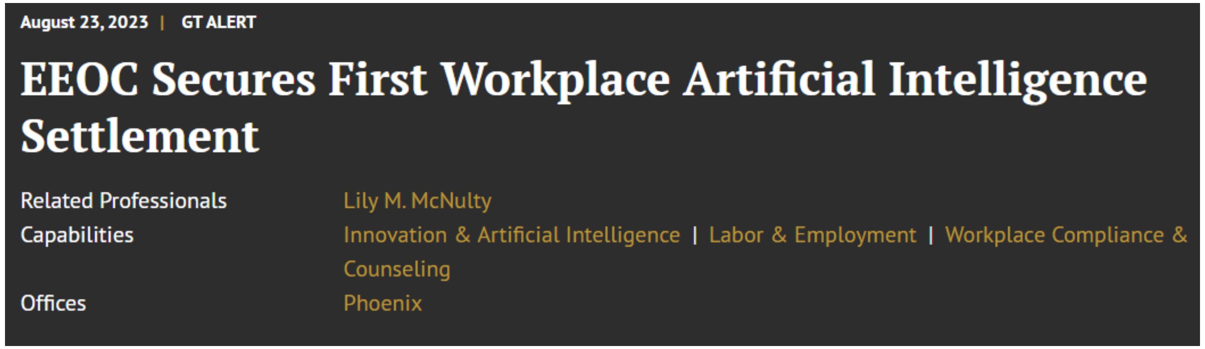
# But it can also go pretty badly wrong...



## Air Canada must pay damages after chatbot lies to grieving passenger about discount

Airline tried arguing virtual assistant was solely responsible for its own actions

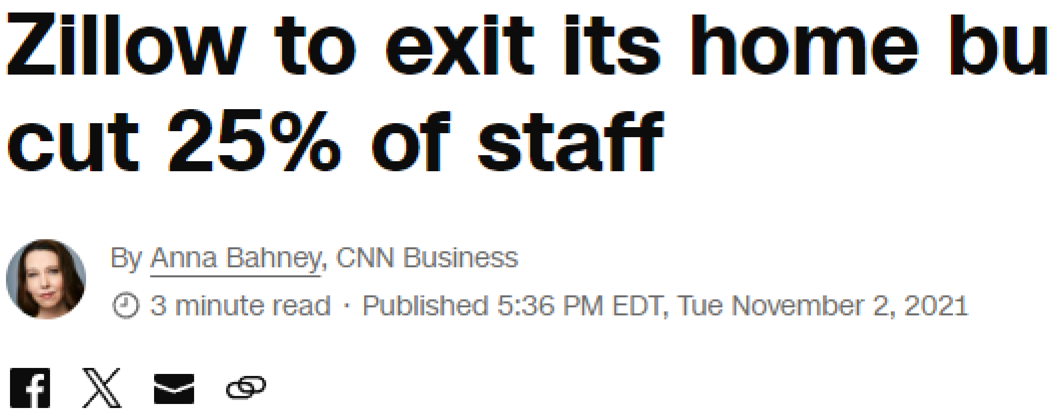
Katyanna Quach Thu 15 Feb 2024 // 21:50 UTC



August 23, 2023 | GT ALERT

## EEOC Secures First Workplace Artificial Intelligence Settlement

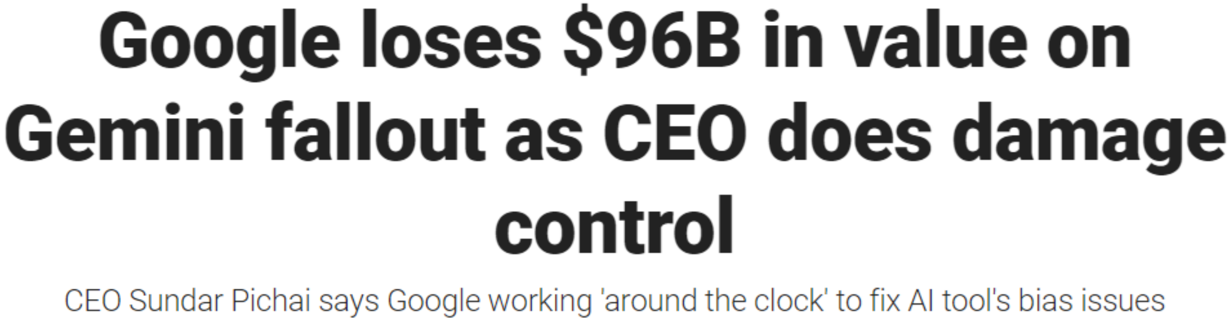
| | |
|---|---|
| Related Professionals | Lily M. McNulty |
| Capabilities | Innovation & Artificial Intelligence \| Labor & Employment \| Workplace Compliance & Counseling |
| Offices | Phoenix |



## Zillow to exit its home buying business, cut 25% of staff

By Anna Bahney, CNN Business

3 minute read · Published 5:36 PM EDT, Tue November 2, 2021



## Google loses $96B in value on Gemini fallout as CEO does damage control

CEO Sundar Pichai says Google working 'around the clock' to fix AI tool's bias issues

AI is not **Magic**

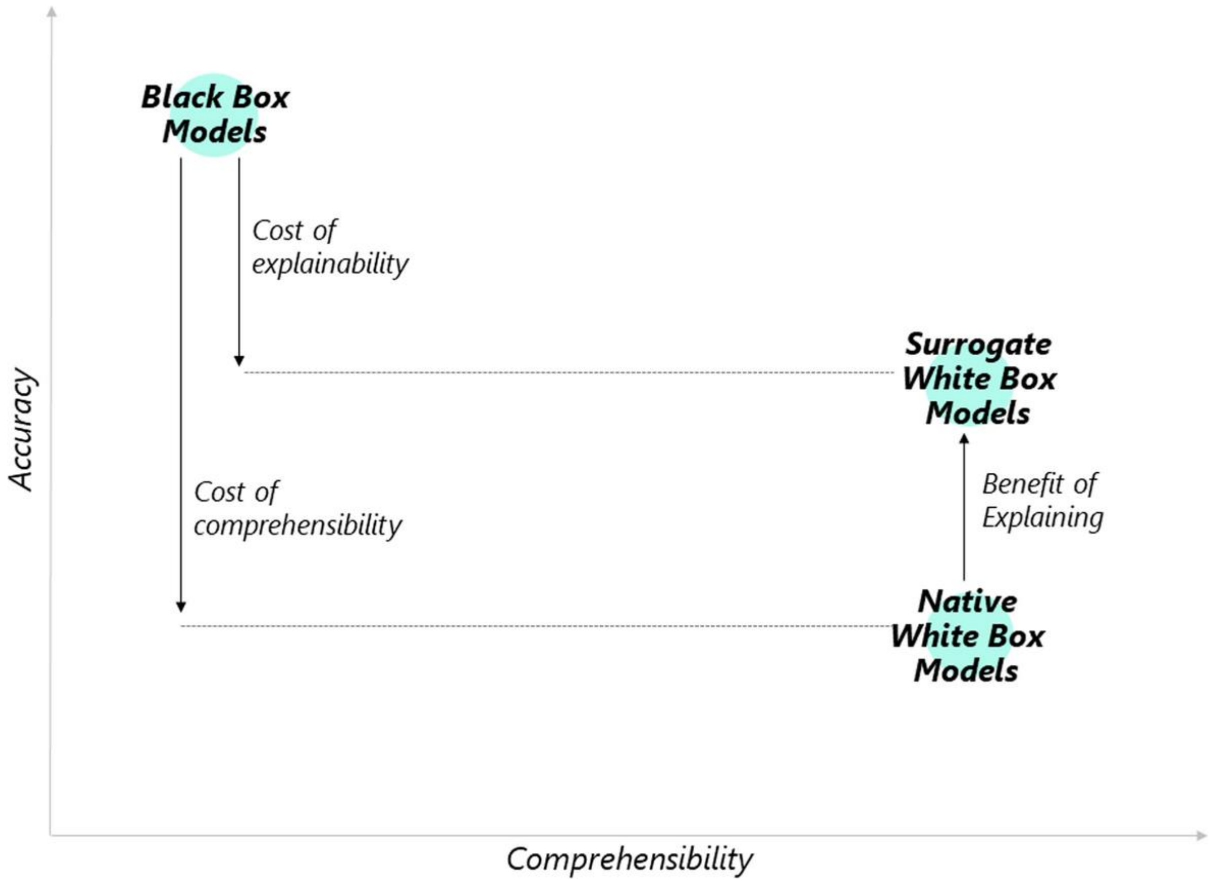
It is an **high quality parrot**

It needs **high quality training data**

# What happens your data isn't ready?

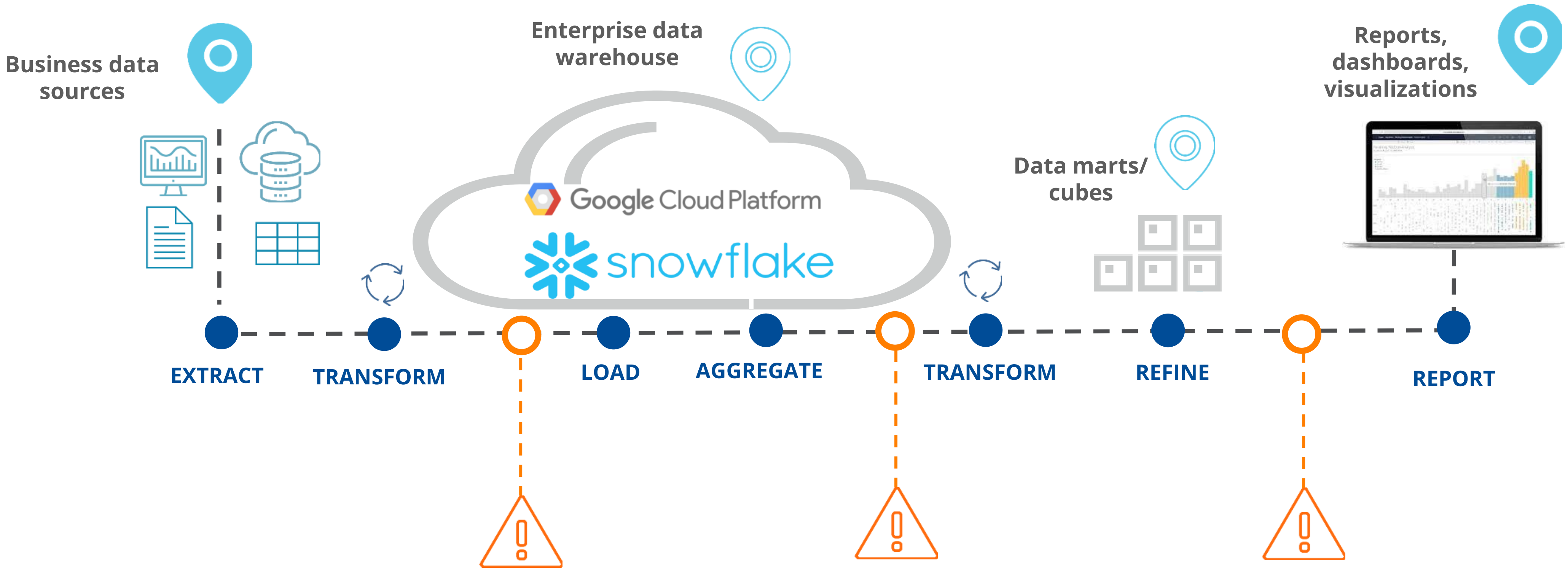
1. Errors introduced early result in biased or poorly trained models
   - Training is expensive and can be hard to validate
2. In the worst case, we cannot detect it until production
   - Learning models can obscure quality issues with complex pseudo function
3. Compliance issues surfacing late can be fatal to AI initiatives

- Can your data prove compliance?



Source: Harvard Business Review

# The race is on to find the data errors



?

Did the problem originate in the source data?

Was there an issue with a data load?

?

Did a transformation job go wrong?

Did a job fail to run or run too many times?

Were there issues with the transformation logic?

?

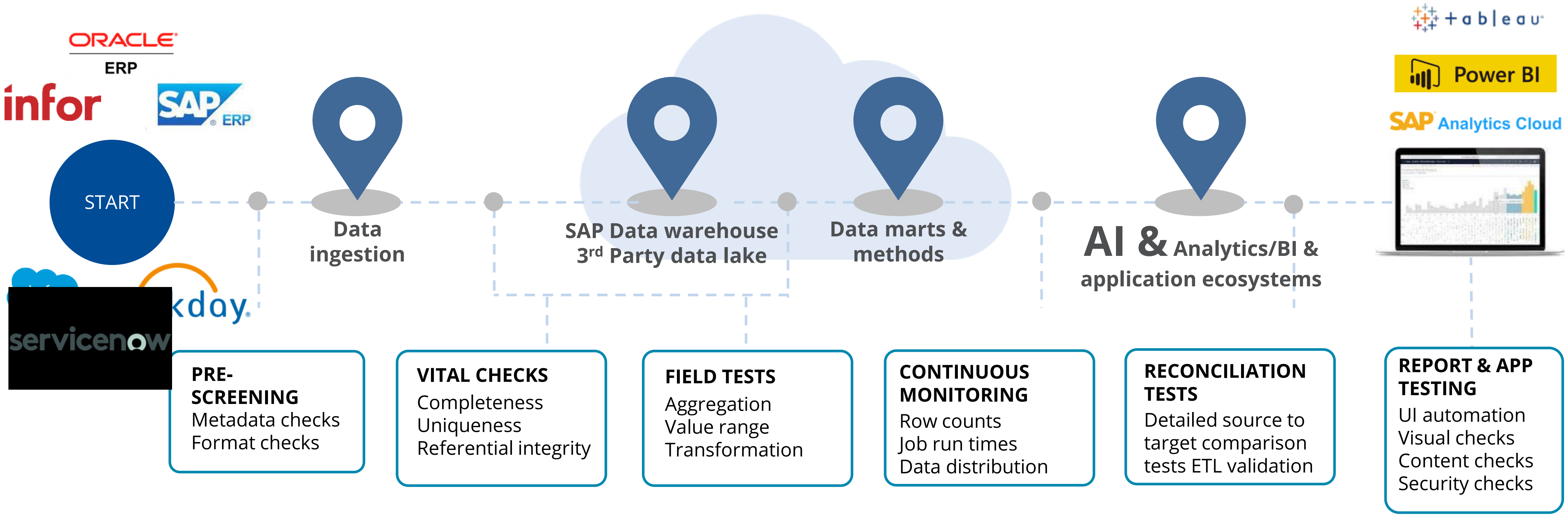
Is the report pulling from the right data mart?

Is there a problem with the report logic?

Is the report rendering incorrectly?

# Deliver trustworthy data through a Complex Process

## Example scenario: Data Pipeline for analytics and dashboards



**PRE-SCREENING**
Metadata checks
Format checks

**VITAL CHECKS**
Completeness
Uniqueness
Referential integrity

**FIELD TESTS**
Aggregation
Value range
Transformation

**CONTINUOUS MONITORING**
Row counts
Job run times
Data distribution

**RECONCILIATION TESTS**
Detailed source to target comparison tests ETL validation

**REPORT & APP TESTING**
UI automation
Visual checks
Content checks
Security checks

# Improving your data quality improves your dev time

Before:

- 2 Months dev effort
- Limited progress

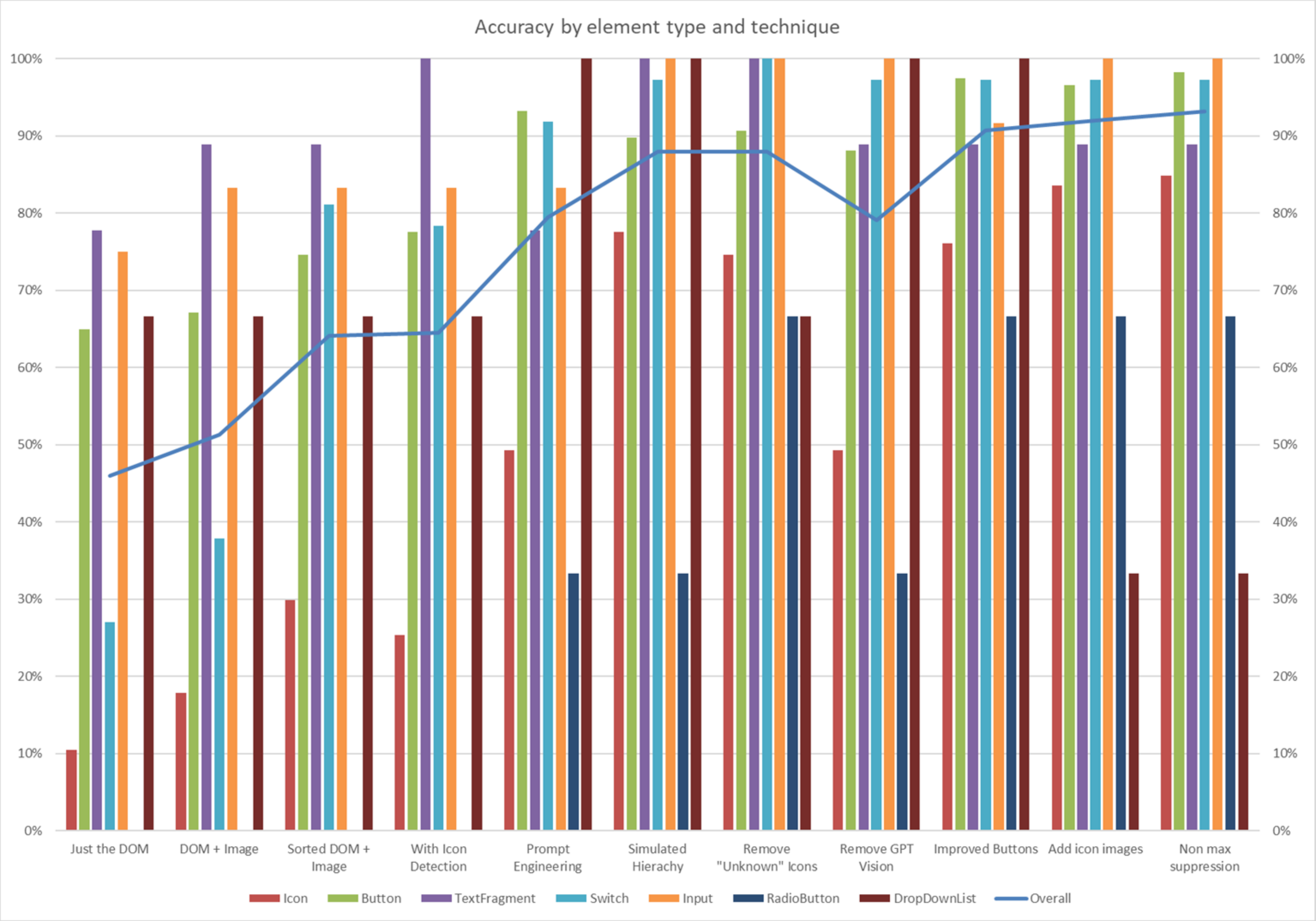
Actions:

❑Cleanse input data

❑Re-categorise and validate

After:

✓1 week from 46% to 93%



# Testing AI Challenges

UNPREDICTABILITY: CHALLENGE OF TESTING AI-GENERATED CONTENT, WHICH CAN BE UNPREDICTABLE AND VARIABLE.

LACK OF GROUND TRUTH: THE DIFFICULTY OF ESTABLISHING GROUND TRUTH (YOUR BENCHMARKS) FOR AI-GENERATED CONTENT, MAKING IT HARD TO EVALUATE ACCURACY.

CONTEXTUAL UNDERSTANDING: THERE IS A NEED FOR TESTERS TO UNDERSTAND THE CONTEXT IN WHICH AI-GENERATED CONTENT IS BEING USED.

BIAS AND FAIRNESS: THE IMPORTANCE OF TESTING FOR BIAS AND FAIRNESS IN AI-GENERATED CONTENT.

# Approaches for Testing AI

1) **Black Box Testing:** Use black box testing to evaluate AI-generated content without knowledge of the underlying model.
2) White Box Testing: Use white box testing to evaluate AI-generated content with knowledge of the underlying model.
3) Hybrid Approaches: Hybrid approaches that combine black box and white box testing.
4) Evaluation Metrics: Use evaluation metrics such as accuracy, precision, recall, and F1 score to assess AI-generated content.
5) Human Evaluation: *Automation* of the human evaluation in assessing the quality and relevance of AI-generated content.

# Tools and Techniques for Testing AI

**Manual: Human-in-the-Loop Testing:** Use human-in-the-loop testing to evaluate AI-generated content

**Better:**

**Testing Frameworks**: Testing frameworks such as PyTorch, TensorFlow, Keras, and focused frameworks like Tricentis

**Best:**

**Automated Testing Tools**: Tricentis automated testing tools.

# Deeper AI Testing Use Cases

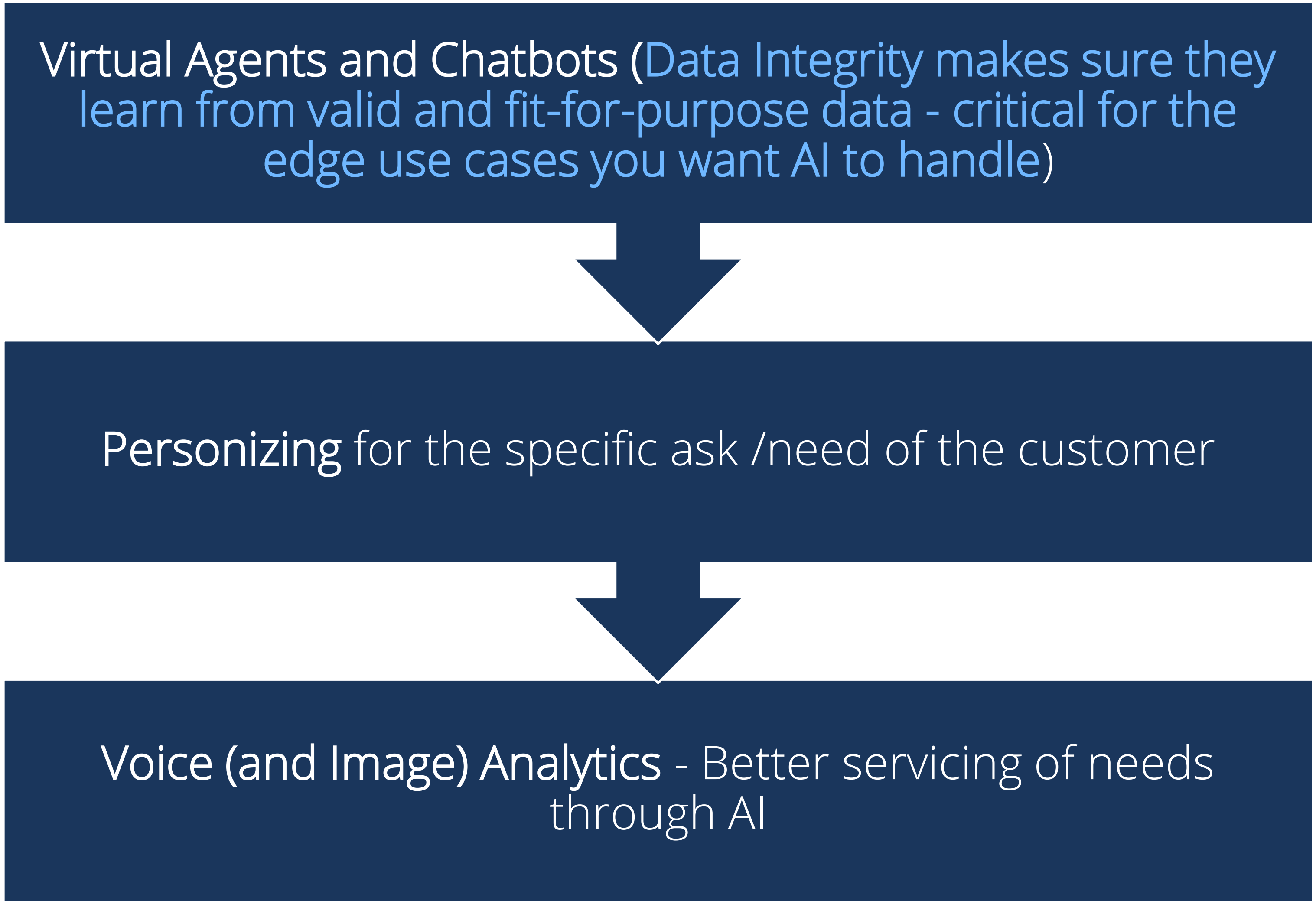
# AI Benefits from Data Integrity

Create a solid data foundation for your analytics and AI projects by feeding them trustworthy data in a simple, efficient and cost-effective way. Use clean, fit-for-purpose data

- **3 major areas for AI impacts on a business**
  - Gen AI:
    - Improving the customer experience
    - Employee productivity boosted with AI
  - ML/Predictive AI: Optimizing Business Operations Outcomes
    - Data Migrations
    - Innovation
    - Compliance

# Improving the customer experience: (Customer Contact) And Employee productivity boosted with AI (Generative AI)

Create and Validate Content data integrity with automated, end to end and continuous data validations for your employee's AI processes



Virtual Agents and Chatbots (Data Integrity makes sure they learn from valid and fit-for-purpose data - critical for the edge use cases you want AI to handle)

Personizing for the specific ask /need of the customer

Voice (and Image) Analytics - Better servicing of needs through AI

# Optimizing Business Operation's Outcomes

- **AI/ML**
  - **Risk**
    - Fraud Detection
    - Compliance requirements
  - Predictive Innovation
    - Business Process Optimization
  - Gen Innovation
    - Intelligent Document Processing

# Optimizing Business Operation's Outcomes – Risk / Compliance

- Example Banking Compliance
  - AML & AML + KYC compliance
    - Anti – Money Laundering and Adversarial Machine Learning
    - Compliance reporting with AI.ML produced data
  - Backdoor attacks can happen purpose or by accident

Integrity of the Data in the Models

Includes:

1. Schema and Metadata Checks
2. Parsing Checks
3. Clean-Label and Backdoor Poisoning

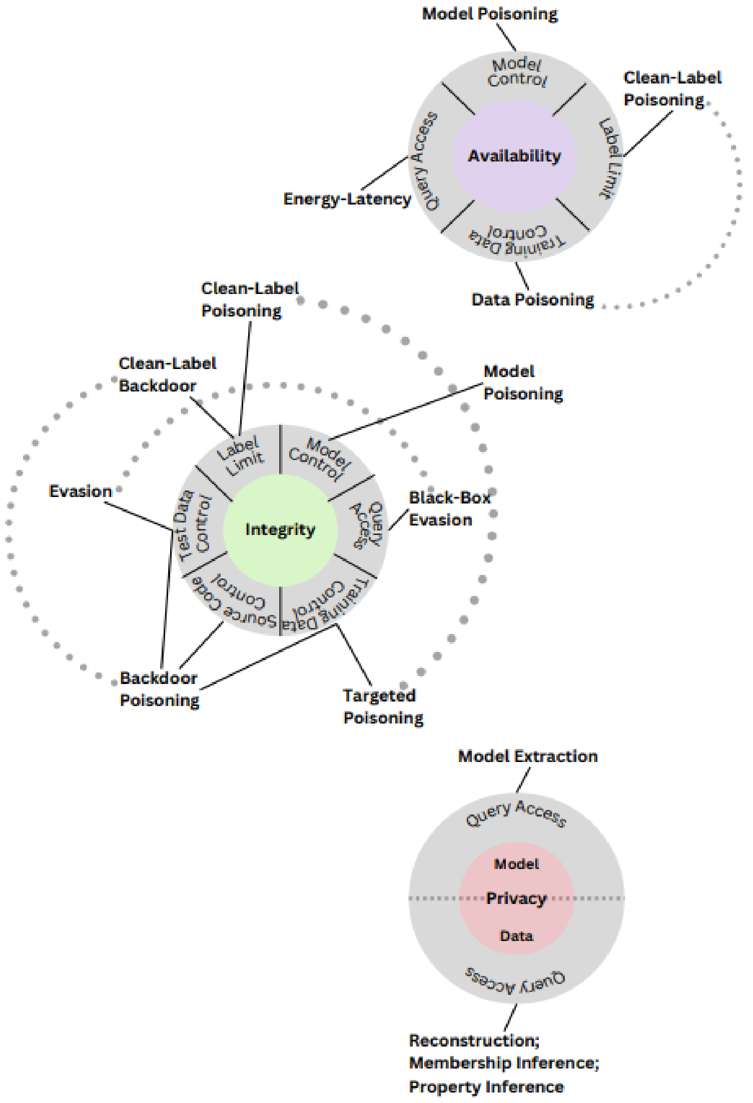


**Figure 1. Taxonomy of attacks on Predictive AI systems.**

NIST Trustworthy and Responsible AI NIST AI 100-2e2023 Diagram

# Logistics Company DI Success Example

## SITUATION

- Validating all  data movements across heterogenous data sources was time consuming
- Manual data integrity testing offered limited test coverage and cost the team hundreds of hours
- Ensuring accurate continuous integration checks with the regular ETL process  was not scalable
- Difficulty Properly validating against data sources to ensure the accuracy of critical business reports
- Could not compare complex validations such as JSON results returned by an API call against the data sources

## NEED

- The company now ensures data quality amongst their daily data movements using their ETL tool throughout CI/CD pipeline. Tricentis Data Integrity automatically triggers their Azure pipeline jobs once the data gets moved by their ETL job

- Tricentis Data Integrity then calls the execution lists to validate the entire data set against source and target schema. A consolidated report is sent that provides an overall health status to stakeholders

## RESULTS

- 90% increase in testing efficiency
- Billions of records validated through automation strategy
- 100% coverage validating structured and semi-structured datasets

# An AI/ML Data Integrity Story

- Major Pharma Vaccines Group
  - Problems with ML models not leading innovation decisions correctly
    - Non-Curated data used for model training
    - Non-curated data used for model deployment
      - Bias was way off expectations
  - Why?
    - A few folks checking the parsing and completeness (fit for purpose) of gigantic data sets
    - Only manually Spot Checking the data (manual stare and compare) at each stage of ML processes
  - Solution
    - End to End Validation to verify the changes to data sets where expected, conforming and regression checked against ALL other data in the ENTIRE process.
    - Automation allowed 90% of the data to be checked, even with large datasets
    - Continuously checked, with embedding in the AI/ML Azure processes, Databricks and PowerBI tooling.
  - Results!
    - $1B Vaccine at market success!

# Major Pharmacy Company Optimizes their AI/ML Initiatives

## SITUATION

- Embarking on AI/Ml projects without a data testing solution introduced
- Too much manual testing, customer was manually spot checking
- ML models not leading innovation decisions correctly
- Non-curated data used for model training and deployment

## NEED

- Looking for a data testing tool that was automated, end-to-end, and continuous

## RESULTS

- Saved money and time moving to automation
- Made sure data was validated throughout the migration process
- Testing continuously to find defects before production

**90%**

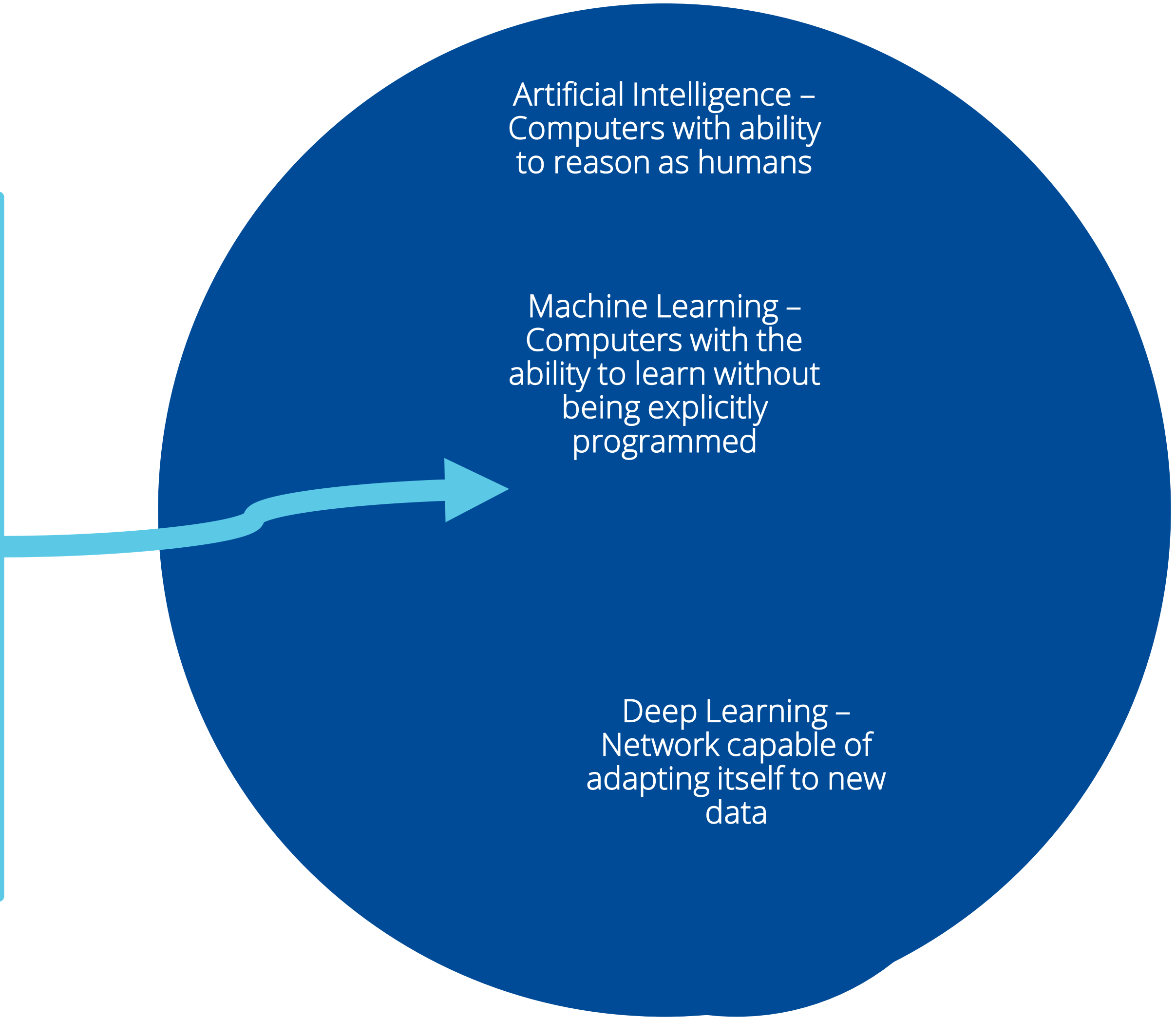
**Of the data was able to be checked including metadata**

**1B$**

**Vaccine at market success**

# Where Data Integrity fits in AI/ML

Data Integrity capabilities in this context our target today.
-Focus on Machine Learning
- Focus on Predictive Models with Supervised Learning



Artificial Intelligence – Computers with ability to reason as humans

Machine Learning – Computers with the ability to learn without being explicitly programmed

Deep Learning – Network capable of adapting itself to new data

<u>(Predictive) Discriminate Models</u> are:

- Regression
- Classification
- Logistic Regression
- Support Vectors Methods
- Convolutional Neural Networks
- Reinforcement Learning
- Federated Learning
- Ensemble Learning
- xgBoost

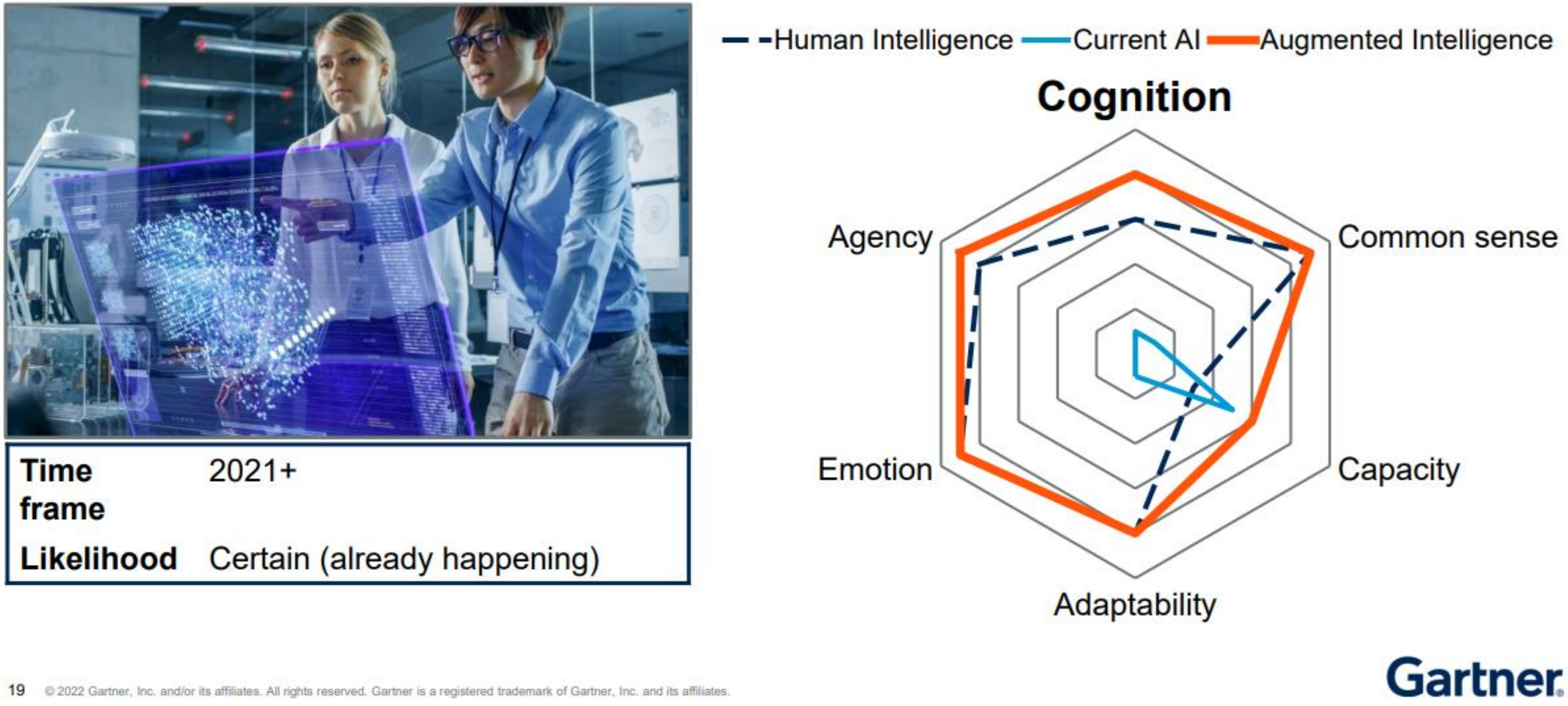
Point □ Labeled data most important here - Supervised

<u>Generative Models</u> are:

- Gan – Gen Adversarial Models
- LLM – Large Language Models

Point □ Unlabeled data drives these - Unsupervised

# Augmented Intelligence: Complementing Human Strengths Using Automated Data Integrity as the Humans



| | |
|---|---|
| **Time frame** | 2021+ |
| **Likelihood** | Certain (already happening) |

19 © 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

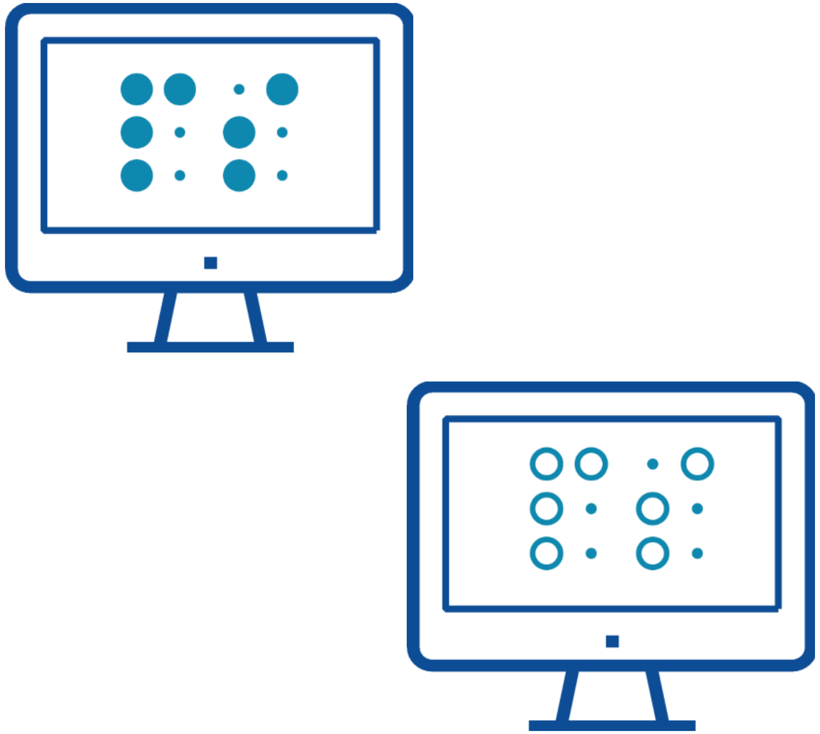
Gartner

# Manual “stare and compare” is slow and doesn’t scale.

And is not a great use of your team’s brainpower.

They are Data Scientists and Engineers not Janitors

10^9th power is 1bil records! Years to manually check!



# Required to ensure data integrity Trust □ A data TESTING solution that's...

**Includes data, UI, and API testing for any data type — across your entire landscape.**

End-to-end

**Automation Augments AI with Automated Humans with Training data coverage > 90%**

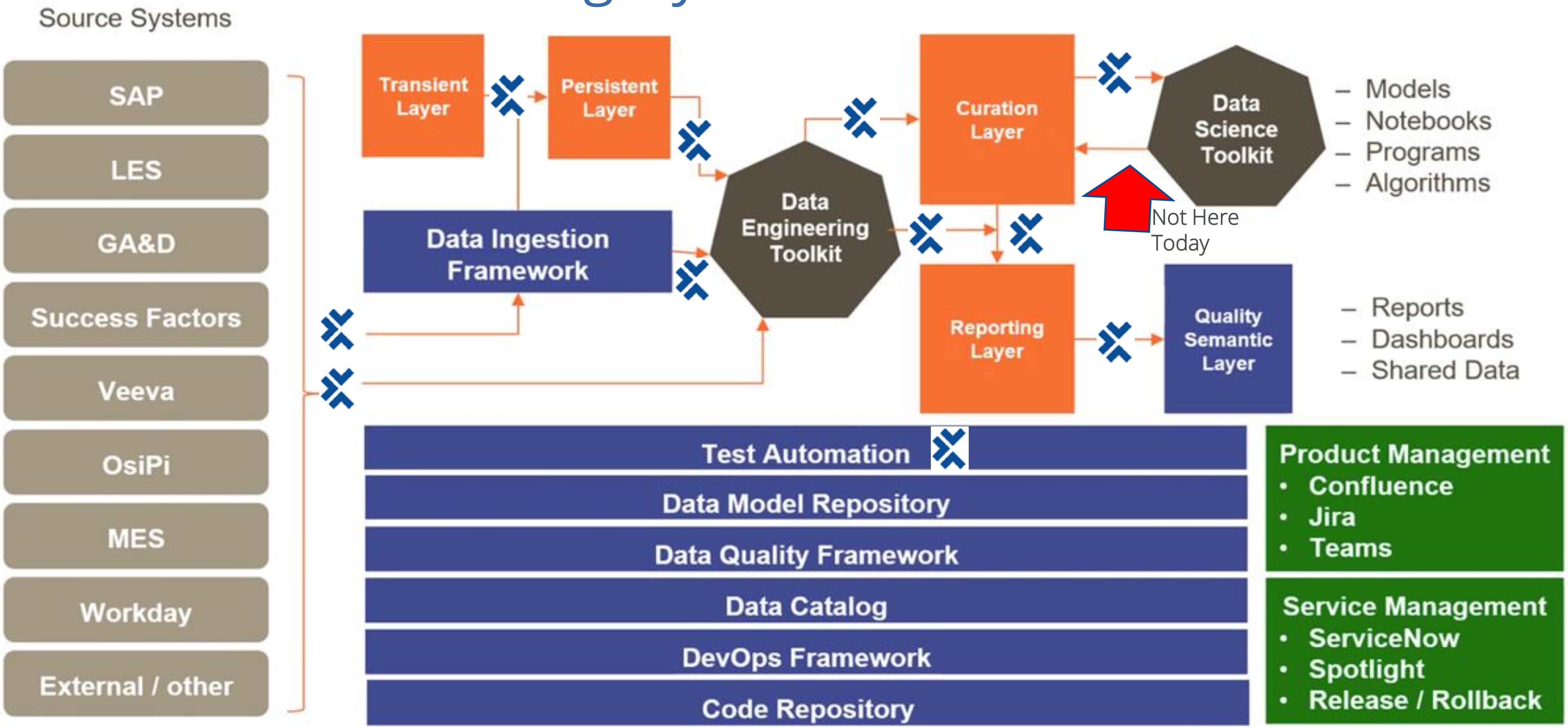
Automated

**Utilize DevOps □ DataOps □ MLOps □ capabilitiess for Continuous TRAINING and DRIFT FIX**

Continuous

# Example Reference Architecture for ML with Data Integrity

| | | | |
|---|---|---|---|
| 🟫 | Source Data | ⬣ | D&A Governed Toolkits |
| 🟧 | Cloud Data Stores | 🟩 | Plan, Monitor, Manage & Control |
| 🟦 | D&A Governed Capabilities | | |



Source Systems

- SAP
- LES
- GA&D
- Success Factors
- Veeva
- OsiPi
- MES
- Workday
- External / other

Transient Layer

Persistent Layer

Data Ingestion Framework

Data Engineering Toolkit

Curation Layer

Reporting Layer

Data Science Toolkit

- Models
- Notebooks
- Programs
- Algorithms

Not Here Today

Quality Semantic Layer

- Reports
- Dashboards
- Shared Data

Test Automation

Data Model Repository

Data Quality Framework

Data Catalog

DevOps Framework

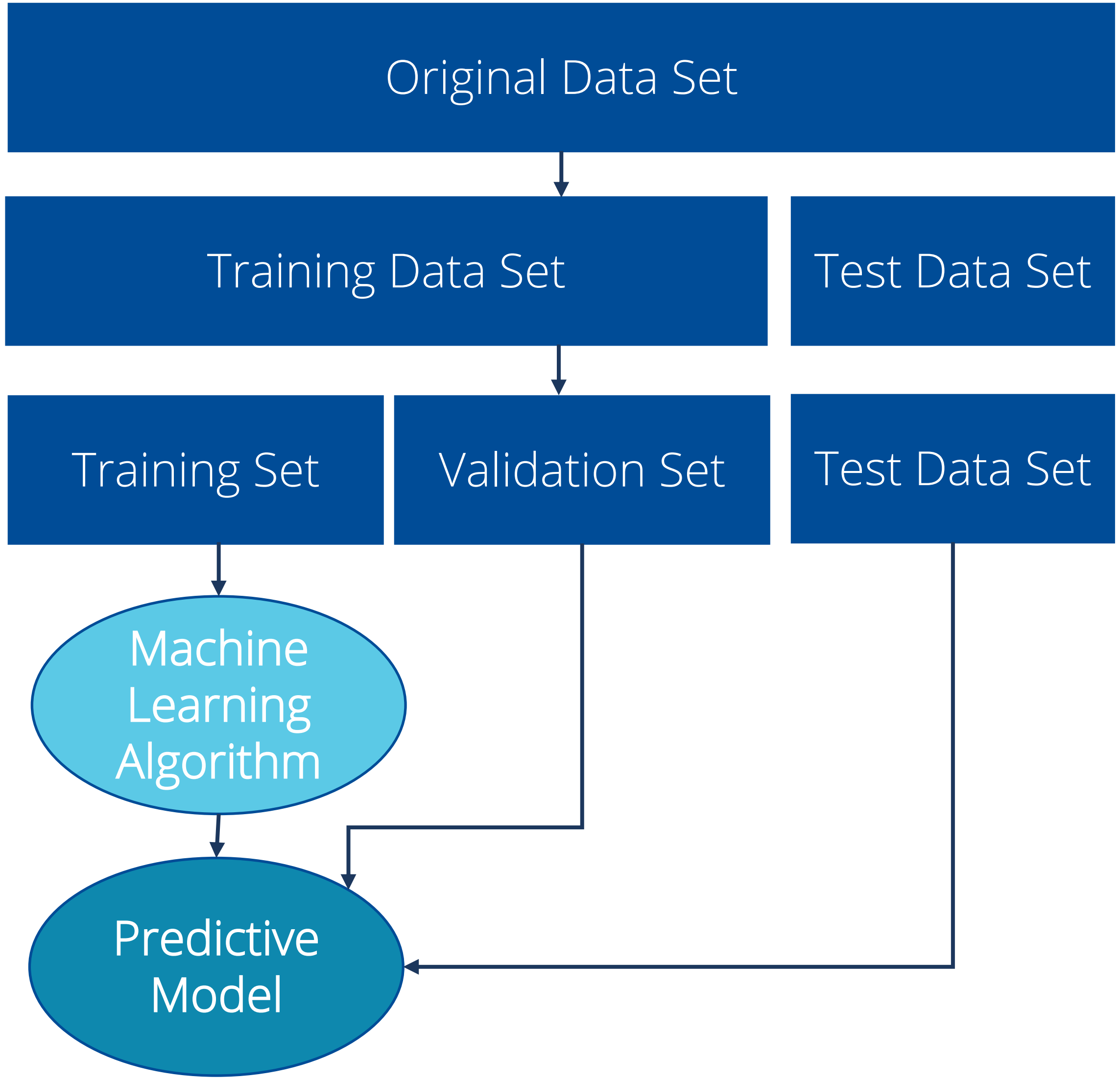
Code Repository

**Product Management**
- Confluence
- Jira
- Teams

**Service Management**
- ServiceNow
- Spotlight
- Release / Rollback

# How we can assist with Training Data

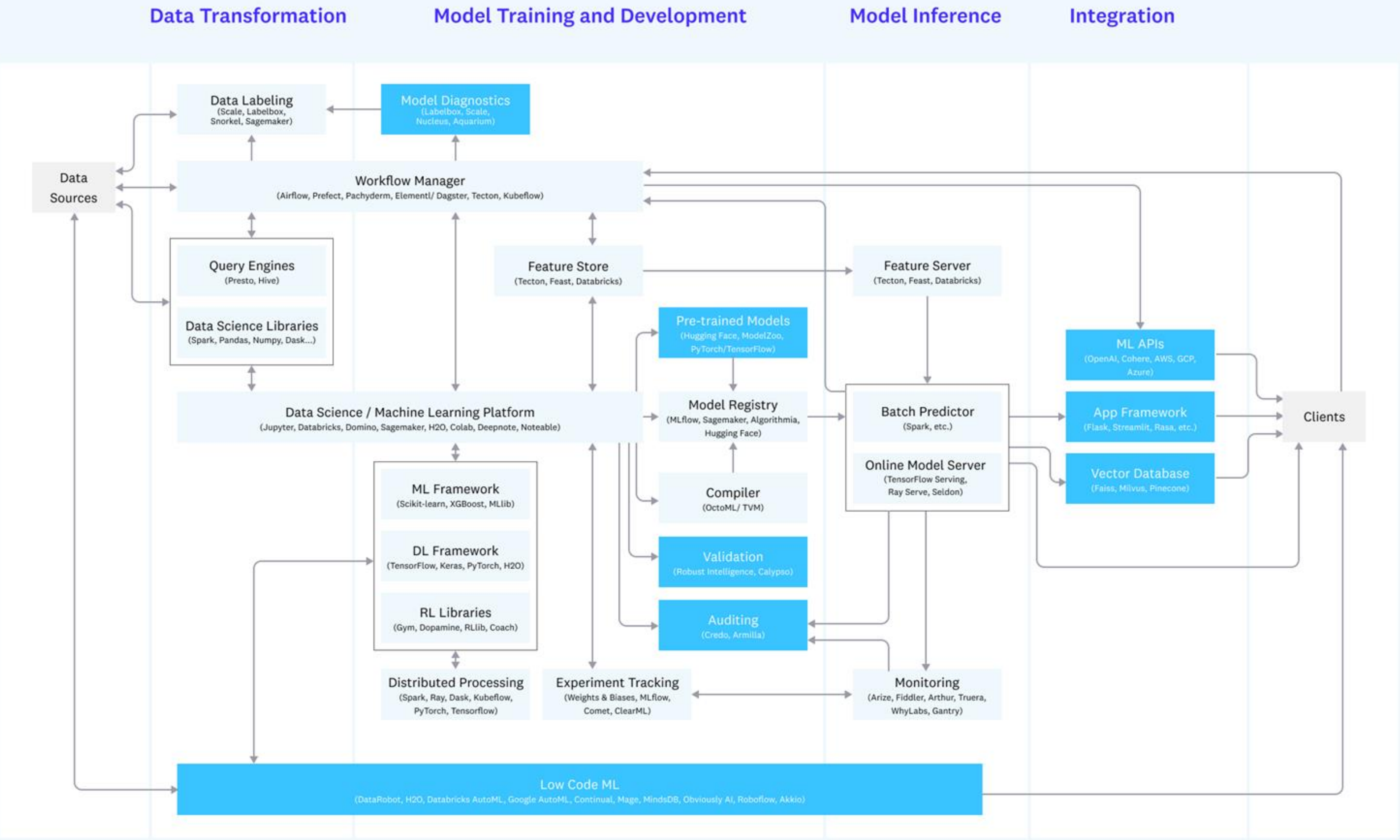
- Testing Data Can be a great primer for Training data and Test Data
- Feature engineering enhanced by great data and business analysts understanding
- If you get public datasets they are often laden with data problems
  - Ex. Our CMS data set for Snowflake



# Migrating to the new Emerging Architectures for Modern Data Infrastructure requires Data Integrity

Emerging Architectures for Modern Data Infrastructure Andreessen Horowitz

## Blueprint 3: Artificial Intelligence and Machine Learning


Data Transformation
Model Training and Development
Model Inference
Integration
Data Labeling
(Scale, Labelbox, Snorkel, Sagemaker)
Model Diagnostics
(Labelbox, Scale, Nucleus, Aquarium)
Data Sources
Workflow Manager
(Airflow, Prefect, Pachyderm, Elementl/ Dagster, Tecton, Kubeflow)
Query Engines
(Presto, Hive)
Data Science Libraries
(Spark, Pandas, Numpy, Dask...)
Feature Store
(Tecton, Feast, Databricks)
Feature Server
(Tecton, Feast, Databricks)
Pre-trained Models
(Hugging Face, ModelZoo, PyTorch/TensorFlow)
ML APIs
(OpenAI, Cohere, AWS, GCP, Azure)
Data Science / Machine Learning Platform
(Jupyter, Databricks, Domino, Sagemaker, H2O, Colab, Deepnote, Noteable)
Model Registry
(MLflow, Sagemaker, Algorithmia, Hugging Face)
Batch Predictor
(Spark, etc.)
App Framework
(Flask, Streamlit, Rasa, etc.)
Clients
Online Model Server
(TensorFlow Serving, Ray Serve, Seldon)
Vector Database
(Faiss, Milvus, Pinecone)
ML Framework
(Scikit-learn, XGBoost, MLlib)
Compiler
(OctoML/ TVM)
DL Framework
(TensorFlow, Keras, PyTorch, H2O)
Validation
(Robust Intelligence, Calypso)
RL Libraries
(Gym, Dopamine, RLlib, Coach)
Auditing
(Credo, Armilla)
Distributed Processing
(Spark, Ray, Dask, Kubeflow, PyTorch, Tensorflow)
Experiment Tracking
(Weights & Biases, MLflow, Comet, ClearML)
Monitoring
(Arize, Fiddler, Arthur, Truera, WhyLabs, Gantry)
Low Code ML
(DataRobot, H2O, Databricks AutoML, Google AutoML, Continual, Mage, MindsDB, Obviously AI, Roboflow, Akkio)

# Data Integrity Benefits for AI - Recap

1. Feature Engineering augmented with Application Test Parameters
    - Business Value associated with all AI/ML comes from the quality of Features and Hyperparameters
2. Training Data augmented with Test Data from Data and Application's Tests
    - Efficient Creation of Test Data for testing, utilized for training data, can decrease TTM for AI/ML solutions
3. Data Migrations from Unified Data Model 2.0 to ML Data Model 2.0
    - Move data for AI/ML at 2x the speed
4. Validation of integrated data models into Data Science
    - A solid automated MLOps process will ensure results and TTM
5. Validation of pipeline for delivery of Data Science results
    - See #4

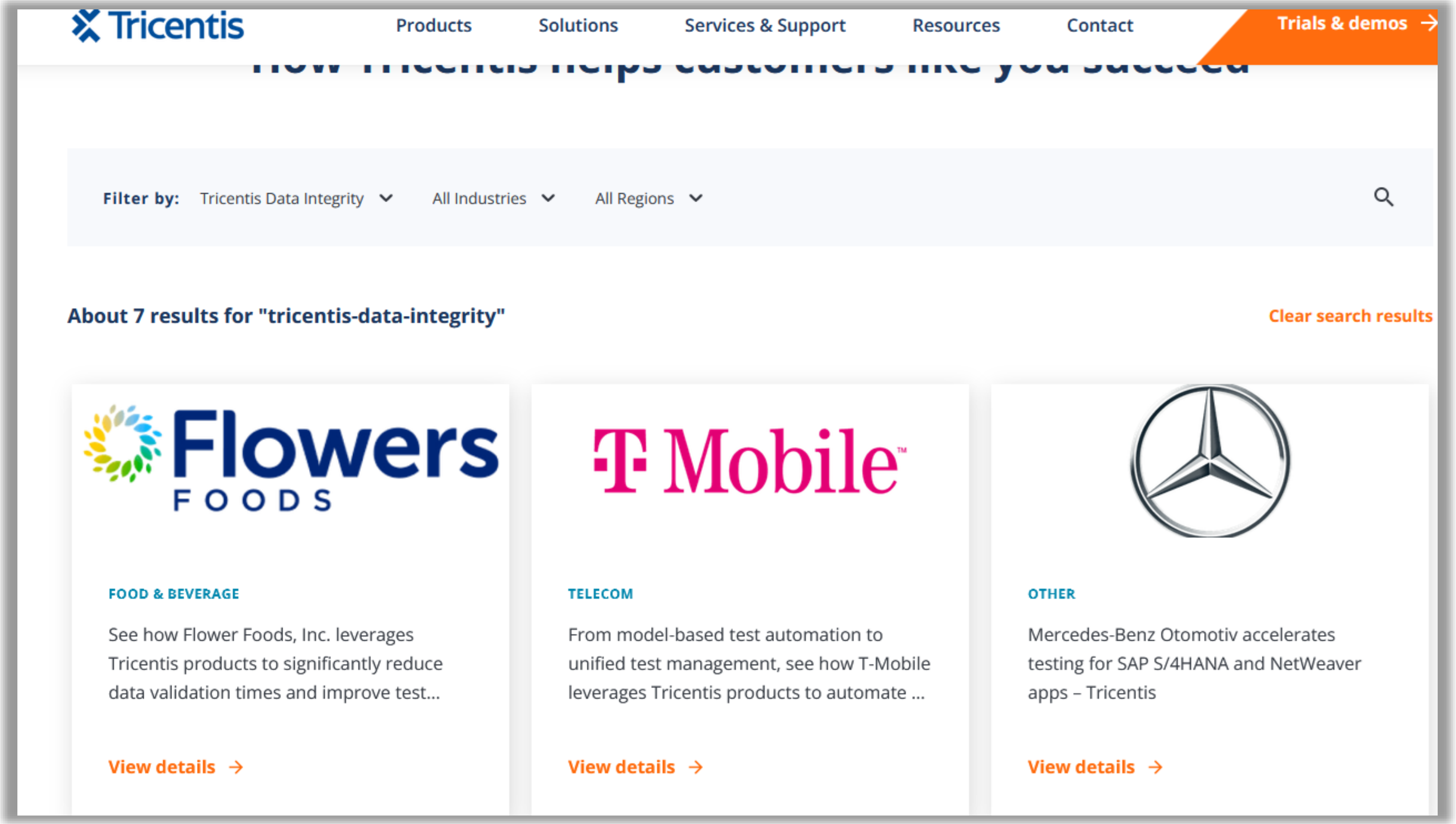
# Thank You!

# Latest SAP Data Integrity Super Use Case (For our SAP friends)

Tricentis
Data Integrity

# SAP EDIT – ECC to HANA Migration Testing

- Flowers Foods Case Study
- After implementing Tricentis Data Integrity, the Flowers team fulfilled several key objectives: they were able to build automation to ensure the integrity of data as it traveled across multiple systems during the data migration from ECC to S4 cutting across several functional domains. Their automation test designer was able to build and execute the complex, end-to-end test case within a few hours, an improvement over their manual total cycle by over 60%.



Filter by: Tricentis Data Integrity All Industries All Regions

About 7 results for "tricentis-data-integrity"

Clear search results

FOOD & BEVERAGE

See how Flower Foods, Inc. leverages Tricentis products to significantly reduce data validation times and improve test...

View details →

TELECOM

From model-based test automation to unified test management, see how T-Mobile leverages Tricentis products to automate ...

View details →

OTHER

Mercedes-Benz Otomotiv accelerates testing for SAP S/4HANA and NetWeaver apps – Tricentis

View details →