OneModel Academy

One AI

Security & One AI

Machine Learning

Hayley Bresina
One AI Client Enablement

31 May 2024

Topics Covered

- Security within machine learning model creating, editing, & managing
- Security within storyboards with model insights & components

Learning Outcomes

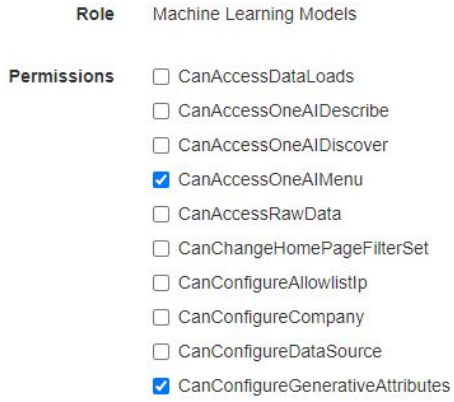
You will:

- Understand the ethical & strategic considerations of promoting full data access for users involved in building or managing machine learning models in One AI
- Become familiar with the necessary application access roles for effectively using machine learning in One AI
- Learn scenarios where data access roles are not fully recognized during the model creation & management process
- Understand that storyboards with machine learning insights fully comply with One Model's role-based security, so viewers don't need full data access

Security in Model Creation & Management

Security in Model Creation & Management

- ML model building & management is intended for users with **full data access**
  - Necessary for interpreting models
  - Essential for making informed decisions during the model-building, evaluation, & troubleshooting processes
  - Helps model creators identify potential biases, fairness concerns, or ethical implications associated with the data
- **CanAccessOneAIMenu** application access role is required; **CanConfigureOneAIGenerativeAttributes** is optional



Security in Model Creation & Management

- When building ML models, users can view & use every metric, dimension, & column that exists within your One Model site, **regardless of data access role**
  - Unpermitted columns can be included as core attributes
    - Will be made 100% null & automatically dropped
  - Unpermitted metrics can be used as the prediction or population metric
    - Model can be created, but will error while running
    - Models always run as the user that created the model
  - Unpermitted metrics can be used to create generative attributes
    - If selected, model can be created, but will error while running

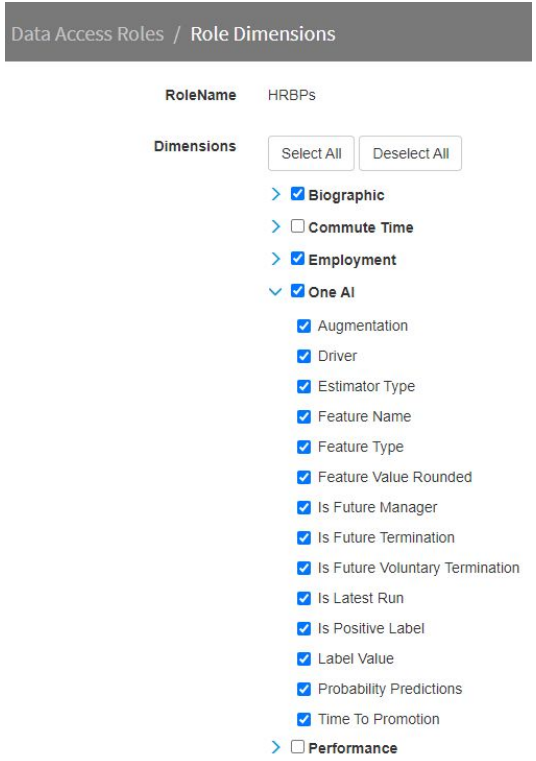
Security in Model Creation & Management

- When building ML models, users can view & use every metric, dimension, & column that exists within your One Model site, **regardless of data access role**
  - Users can download the train/rest data & predict data for all ML models in One AI
    - Downloads contain by row data, usually by person_id, with values for each included core attribute
    - Potentially includes generative attributes, salary information, DEI data, performance ratings, & anything else available in One Model
  - Users can view results from every model in One AI - regardless of if they have access to the metrics & columns used to build it
    - From the EDA report, they can perform variable analysis & download correlation for all the columns that were included in the model

Security in Storyboards with ML Components

Security in Storyboards with ML Components

- Role-based security works with ML storyboards the same as it does throughout the rest of One Model
- Users **do not** need full data access to view storyboards that display model insights & results
- One AI machine learning metrics, dimensions, columns, & storyboards are permissioned via data access roles or the storyboard
  - Unpermitted tiles will have a security restriction & data will not be displayed
  - Creators should keep the audience in mind while developing storyboards



OneModel Academy

Thanks for watching!

OneAI