Technical Architecture

Adversarial Playground

Developers / Data Scientists

IDE/ CLI

Containers

Users

Browser

HTTPS 443

GCP

HTTP 80

Source Control

GitHub

Dockerhub

Dockerhub Image Registry

AlexNet Training Image

ResNet Training Image

AlexNet Service Image

ResNet Service Image

Adversarial Playground App Image

Vertex AI

Pull Data

Model Train

AlexNet

ResNet

Three VM Compute Instances

Adversarial Playground App Container

HTTP 8000

HTTP 8000

GCS Bucket

Data & Models

HTTPS 443

HTTPS 443

AlexNet Service Container

ResNet Service Container

HTTPS 443

HTTPS 443