COVID-19 Data Tracker System Architecture (Monolith)

A. Monolith Components:

1. **Express.js Server:**
   - Handles incoming HTTP requests and routes.
   - Manages API endpoints for data extraction and visualization.
2. **Data Processing:**
   - Extracts COVID-19 data from the chosen API source.
   - Parses and processes data for storage and visualization.
3. **Data Storage (MongoDB):**
   - Stores extracted data efficiently.
   - Provides querying capabilities for data retrieval.

B. Database Layer:

1. **MongoDB Collections**
2. **Database Schema:**
   1. **us_daily_data Table:**
      - date (Primary Key)
      - states
      - total_cases
      - total_testing
      - hospitalized_currently
      - in_icu_currently
      - on_ventilator_currently
      - total_deaths
   2. **state_daily_data Table:**
      - date (Primary Key)
      - state
      - total_cases
      - total_testing
      - hospitalized_currently
      - in_icu_currently
      - on_ventilator_currently
      - total_deaths

D. Security Layer

- Use a proper authorization system

H. API Contracts

A. Data Extraction:

1. **National Data**
   a) **Endpoint:** '*/daily*'
   b) **Purpose:** Retrieve historic COVID-19 data for the entire US.
2. **Single-Day Data:**
   a) **Endpoint:** *'/daily/{date}'*
   b) **Purpose:** Retrieve COVID-19 data for a specific date in the US.
3. **Historic Data for a State:**
   a) **Endpoint:** *'/states/{state-code}/daily'*
   b) **Purpose:** Retrieve historic COVID-19 data for a specific state.
4. **Single-Day Data for a State:**
   a) **Endpoint:** *'/states/{state-code}/{date}'*
   b) **Purpose:** Retrieve COVID-19 data for a specific date and state.

*The {date} will have the iso format structure

I. Security Measures and Compliance

- All data is transmitted securely using HTTPS (TLS/SSL).
- Input validation and sanitation are performed to prevent injection attacks.
- There will be a Center Error Handler to ensure security.