Operation Warp Speed

Safeguarding Vaccine Production with Secure Data Pipelines

THE CUSTOMER

Johnson & Johnson's pharmaceutical arm, Janssen, embarked on a global effort to combat the COVID-19 pandemic. To support their goal of supplying one billion doses, an agreement with a contract manufacturer was reached. Large-scale manufacturing of Janssen's vaccine would take place at the contract manufacturing site, which is designed for rapid manufacturing of vaccines and other treatments in large quantities during public health emergencies.

KEY BENEFITS

Accelerated Tech Transfer
Rapidly implement new technologies to expedite vaccine production.

Maintained Quality
Maintain high-quality standards even in a new manufacturing environment.

Optimized Operations
Reduce the need for operators, crucial for maintaining social distancing.

THE PROBLEM

Janssen required access to near real-time data in order to monitor key production and quality metrics and assure the success of each batch. The contract manufacturer's Operational Technology (OT) infrastructure of control systems and data collection is isolated from both internal and outside networks - particularly networks with internet access. The contract manufacturer tasked IxP with creating a secure data pipeline providing this information to Janssen.

THE SOLUTION

A secure and scalable architecture was required to meet Janssen's information needs. Janssen provided an Azure IoT Hub to receive the production and batch data from the contract manufacturer's system. IxP proposed Inductive Automation's Ignition software platform with Cirrus Link's MQTT modiles as the heart of this secure data pipeline. Ignition provided a powerful development environment and support for MQTT messaging. MQTT was ideal for this application as it is deisnged for secure, real-time mission critical data.

The heart of the solution is the Cirrus Link MQTT Transmitter, Distributor and Engine plus the Azure Injector, all running on the Ignition Platform from Inductive Automation.

Utilizing MQTT, IxP established a secure gateway that ensured only Janssen's data is transmitted. The system consists of (3) main companents that work together:
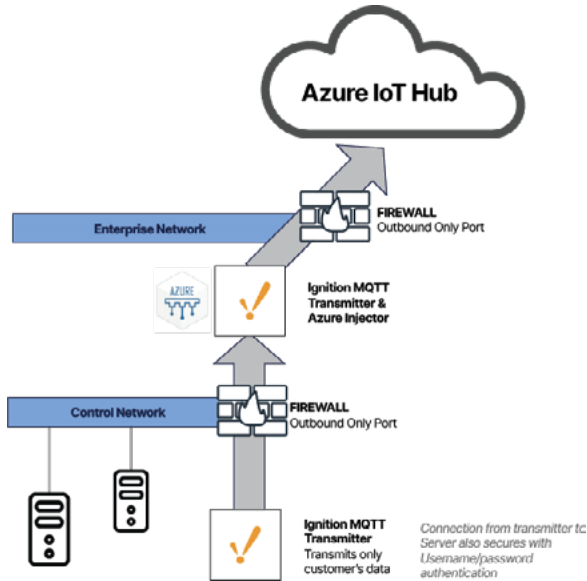
The Ignition Edge Server - acts as the MQTT transmitter at the contract manufacturing plant, gathering on Janssen's key process data directly from the control system and publishing it on the change through an outbound-only port on the control network firewall to the MQTT server. The connection is also secured via user authentication.

The MQTT Server - acts as a secure bridge between the MQTT transmitter and the cloud. It contains a data and history buffer dedicated to Janssen's data. The store and forward capability ensures data is not lost if the connection becomes unavailable. The MQTT server also hosts the Azure Injector.

Cloud Repository - Connection to the cloud is made via an outbound-only port on the enterprise-level firewall. The cloud repository is based on Azura IoT hub and is secure with SSL authentication certificates provided by Janssen.

What is MQTT?

MQTT is a publish/subscribe messaging protocol originally developed over 20 years ago to address the need for lightweight communications over low bandwidth networks. It is based on a topic structure, like a file structure on a computer, and a payload of data. The Sparkplug B specification defines this structure for industrial applications including the topic namespace definition (OT side of things), the payload definition (IT side of things), and the state management for client connections allowing IIoT Applications to talk to one another seamlessly.

MQTT architecture needs three components: MQTT Transmitters - the MQTT Clients that produce the data (usually directly connected to the control or SCADA system) MQTT Engine - the MQTT Clients that consume data MQTT Servers (Distributor Module) - distributes data from the MQTT Transmitters to the MQTT Engine.

Benefits of MQTT:
- Simple and Open
- Bandwidth efficient - up to 90% bandwidth reduction
- State Aware
- Decouples devices from applications
- Utilizes modern TCP/IP security