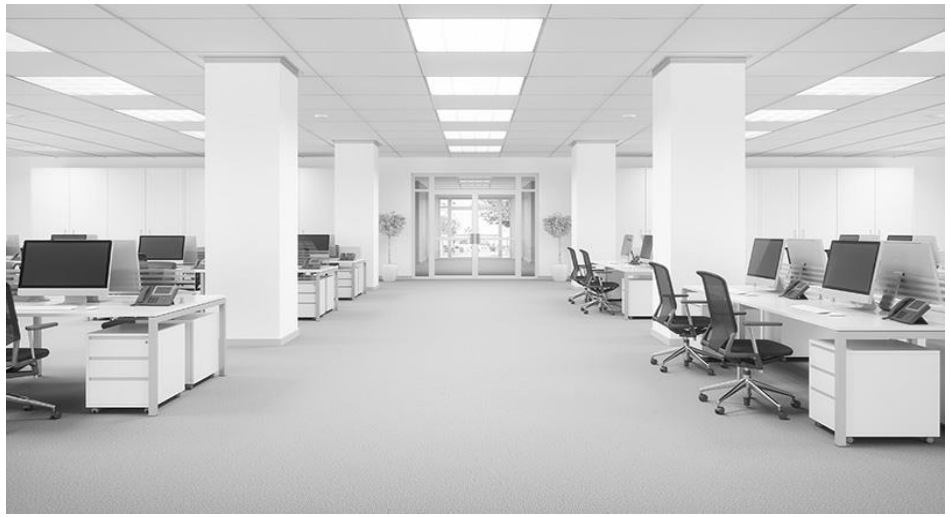
TWINTECH SOLUTIONS

Your Trusted Cyber Partner

Securing Leading Manufacturer Industrial IoT Ecosystem CASE STUDY

Securing Leading Manufacturer Industrial IoT Ecosystem



Business Situation

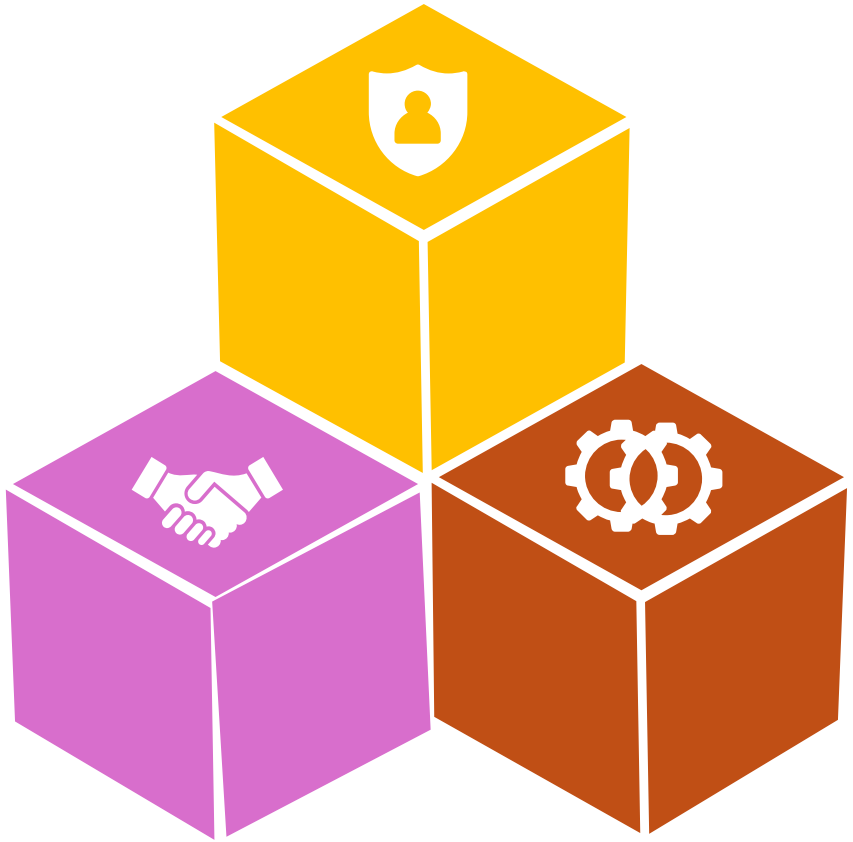
A leading global manufacturer of industrial machinery with a large network of connected factory machines, robots, and sensors. The company needs a proactive approach to identify and address these security gaps before a potential attack disrupts production or compromises valuable intellectual property.

IOT SECURITY

Securing Leading Manufacturer Industrial IoT Ecosystem

1. Industries had deployed a vast network of Internet of Things (IoT) devices to automate their manufacturing processes and improve operational efficiency

IOT SECURITY



2. They lacked a comprehensive security strategy for these devices, raising concerns about potential vulnerabilities and cyberattacks that could disrupt production, damage equipment, or compromise sensitive data.

3. TwinTech need to navigate a vast network of potentially vulnerable devices.

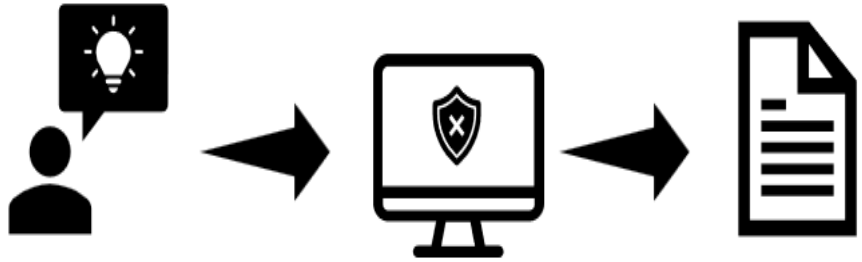
Securing Leading Manufacturer Industrial IoT Ecosystem

TWINTECH SOLUTIONS

TwinTech had a Kick-Off meeting with firm’s CEO and IT Manager to define PenTesting scope

Completed a device walkthrough to gain a comprehensive understanding of the device's workflow and underlying technologies

IOT SECURITY



Securing Leading Manufacturer Industrial IoT Ecosystem

TWINTECH SOLUTIONS

Create a detailed list of all connected devices, including type, firmware version, and function. This helps prioritize vulnerabilities and identify critical systems at risk.

Deploy intrusion prevention systems to identify and block potential attacks proactively.

Threat modeling exposed IoT architecture flaws . We recommended architectural redesign, mitigating vulnerabilities and securing their IoT.

Educate staff on cybersecurity to recognize threats and report suspicious activity.

Update device firmware regularly and enforce strong, unique passwords for all systems.

IOT SECURITY

Securing Leading Manufacturer Industrial IoT Ecosystem

TWINTECH SOLUTIONS

About Client & Client Team

- Leading global manufacturer based out of India .
- Industrial Automation Head

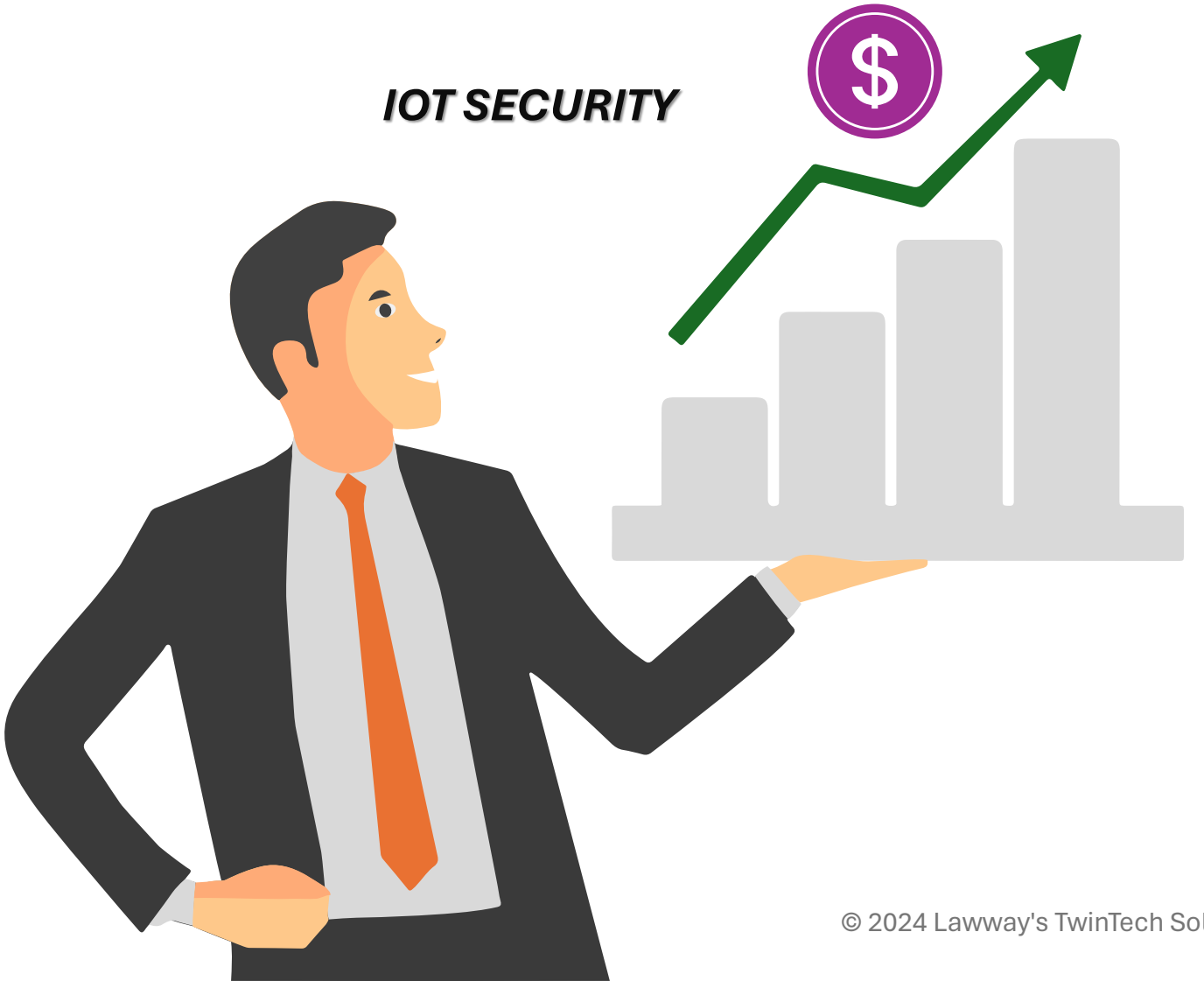
Client Needs

- Ensure compliance with industry IoT security standards.
- Uncover security weaknesses in their vast IoT network.
- Minimize downtime, ensuring smooth production.

Key Strategies Implemented

- Comprehensive Testing Approach
- Map vulnerabilities in their IoT ecosystem
- Proposed architecture changes for enhanced security.
- Business Confidence and International Recognition

Securing Leading Manufacturer Industrial IoT Ecosystem



BENEFITS

- Securing their IoT network helped industry to avoid potential financial losses due to production disruptions, data breaches, or equipment damage caused by cyberattacks.
- Industry significantly improved the security of their industrial IoT network. This reduced the risk of cyberattacks that could disrupt production, damage equipment, or compromise sensitive manufacturing data.
- Ensured the company achieved compliance with industry regulations for IoT device security.