Cyber-Security
Challenges
in Aviation Industry

Overview

XYZ is one of the leading provider in the aviation sector that serves in cargo services, flight operation, air charter services, passenger boarding services and travel, freight control, advisory and consultancy, aircraft preservation and renovation, international flight operation, air supervision, helipad engineering, etc. The airline has a skilled workforce and offers total control and functional back-up to several international schedule / non-scheduled operations.

Business Challenge

XYZ approached Prophaze in order to secure their web application and mobile API, as they were facing few challenges in terms of :

- **Distributed Denial-of-Service (DDoS)** and DoS attacks on network assets at the airport, most notably, Vulnerability Bandwidth Depletion DDoS which made the Denial of Flight Ticket Inventory.
- **Airline Bot Problem** - affected the Scraping of Flights Information, Fraudulent GDS Queries, and Skewed Look to Book Ratio. Cyber attackers used bots to undertake credential cracking and credential stuffing assaults. Personal information

(PII), credit card data, gift card vouchers, and travel history were among the items stolen from user accounts. Illicit virtual currency transfers, such as reward points, wallet money, air miles, gift cards, and so on were also made through those details.
- **API Attacks -** They faced Attacks and data breaches on their poorly protected APIs. Fraudsters took advantage of those API flaws and took over the control of sensitive data.

The Results

Malicious threat actors frequently target this aviation sector in order to gain access to customer information or to extort ransoms. Prophaze's AI/ML-based solutions helped them to protect key assets and thwart advanced attacks. Prophaze WAF simplified their aviation network cybersecurity by protecting web applications, API etc…from known and unknown cyber threats. Prophaze helped to develop cyber security mechanisms in order to mitigate cyber risk as hackers might take advantage of such vulnerable systems that lack proper cybersecurity mechanisms. able to put an immediate stop to entire classes of cybersecurity threats, including account takeovers, web scraping, online frauds, unauthorized vulnerability scans, and application denial of service.