Prophaze's WAF Redefines Aerospace Security Standards

THE CHALLENGE

In the aviation industry, like in many other verticals, Cyber attackers are motivated by financial and political purposes and the desire to obtain sensitive information.

The most seen attack types are Ransomware ,Data Breach , Phishing and DDoS in the aviation industry.

THE CLIENT

The client is one of the largest aerospace and defense organizations in the world. The client wanted to find a cyber security solution that would increase security without reducing the effectiveness of database initiatives that involved outsourcing, software development, and integration testing.

THE SOLUTION

Customer decided to deploy Prophaze Web Application Firewall and was satisfied by its features including AI firewall, DDoS protection, compliance management, virtual patching, incident management and API security.

DevOps teams using Prophaze WAF can receive holistic protection from application vulnerabilities such as data leaks, rate anomaly, malware attacks, exploit bots, zero-day attacks, misconfigured servers, fileless attacks, and scraping bots among others.

The system detects anomalies and protocol IPs in traffic flows via machine language behavior analysis and block DDoS traffic whilst letting valid requests flow through. Additionally, it automatically deploys virtual patching to API, web applications and microservices.

Its multi-tenancy capabilities, which allowed clients to secure data of multiple users on a database and shared application.