

● THREAT ALERT

Ensured **Continuous Availability** with Intelligent Failover and Zero Service Disruption

In April 2023, a sophisticated Layer 7 DDoS attack by Anonymous Sudan targeted six of India's busiest airports, paralyzing operations, disrupting global schedules, and undermining trust in critical aviation infrastructure.

● High-Volume Layer 7 DDoS

● API & Application Overload Attacks

● Continuous Airport Operations Protected

50M+

Malicious Requests Blocked

During peak attack phases
across protected airports

450 Gbps

Attack Volume

Sustained application-layer
traffic flood

0 sec

Downtime

Critical aviation services remained
fully operational

Real-Time

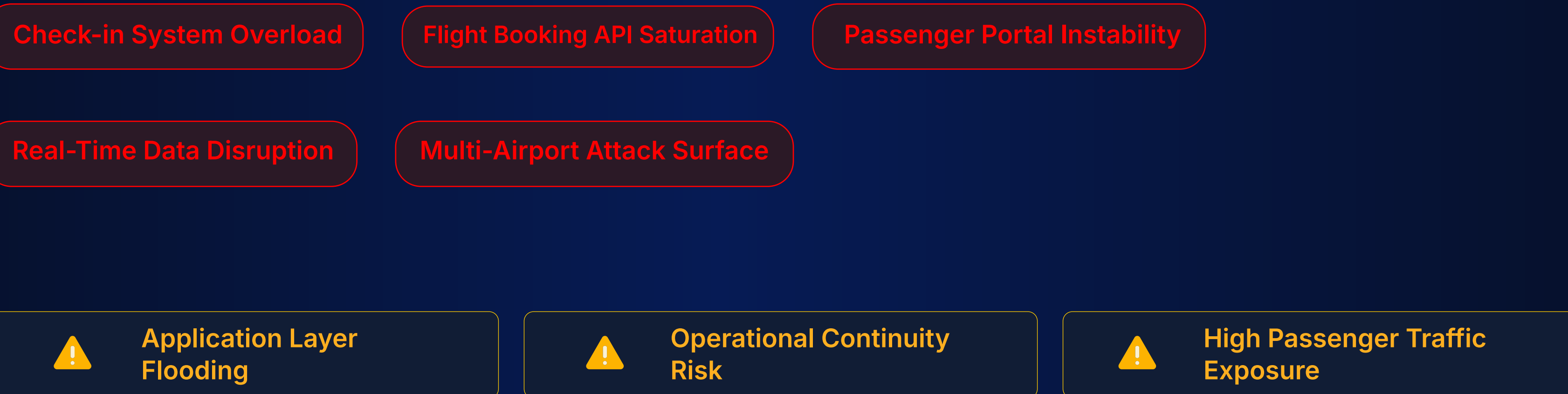
Threat Mitigation

Attacks identified and
neutralized instantly

Aviation Infrastructure Under Coordinated Digital Assault

A major aviation ecosystem faced simultaneous cyberattacks targeting six major airports, disrupting core systems such as flight booking engines, passenger check-in platforms, baggage handling APIs, and real-time flight status services.

The attack exploited application-layer vulnerabilities, overwhelming APIs with high-frequency requests and destabilizing passenger-facing systems during peak operational hours.





Rotating Bot Traffic & Spoofed Requests

Attackers used IP rotation and user-agent spoofing to bypass static defenses and mimic legitimate passenger traffic.



Rapid Request Flooding at Scale

Hundreds of thousands of malicious requests per second overwhelmed airport APIs and backend services



Indistinguishable Traffic Patterns

Malicious and legitimate passenger requests appeared similar, making traditional blocking unsafe.



Critical Operational Impact Risk

Even minor disruptions affected flight schedules, passenger processing, and global airline coordination.

Prophaze WAAP: Multi-Layered Defense for Aviation Infrastructure

Three coordinated capabilities ensured uninterrupted aviation operations and real-time threat mitigation.



Dynamic WAF Scaling & Real-Time DDoS Mitigation

- ✓ Kubernetes-native scaling absorbed massive traffic spikes instantly
- ✓ Blocked over 50 million malicious requests in real time
- ✓ Maintained uninterrupted access to aviation systems
- ✓ Ensured zero service degradation during peak attack load



AI-Powered Traffic Analytics & Anomaly Detection

- ✓ Behavioral analysis distinguished real passengers from bot-driven traffic
- ✓ Machine learning models adapted to evolving attack patterns
- ✓ Real-time threat scoring blocked malicious API requests instantly
- ✓ Protected critical aviation services like booking and check-in systems



CAPTCHA-Less Bot Mitigation System

- ✓ Cookie validation and JavaScript-based verification filters
- ✓ Behavioral pattern analysis for user interaction verification
- ✓ Invisible protection ensured zero friction for real passengers
- ✓ Blocked automated bot traffic without impacting UX

Aviation Systems Remained Fully Operational During Peak Attack Conditions

Here's what was achieved during the attack:



50M+

Malicious Requests Blocked

Neutralized across all targeted aviation endpoints



450 Gbps

Attack Volume Absorbed

Handled without impacting legitimate traffic



0 sec

Zero Downtime

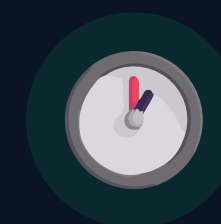
All airport systems remained fully operational



100%

Passenger Service Continuity

No disruption to booking, check-in, or flight operations



Real-Time

Threat Neutralization

Attacks mitigated instantly as they evolved

What Changed When Prophaze Was in Place

✘ BEFORE PROPHAZE	✔ AFTER PROPHAZE
<p>Attack Handling Capability</p> <ul style="list-style-type: none">✘ Legacy aviation security systems struggled to absorb high-volume Layer 7 DDoS attacks, leading to API overload and service instability across airport platforms.	<p>Attack Handling Capability</p> <ul style="list-style-type: none">✔ Prophaze delivered AI-native, real-time mitigation capable of absorbing millions of malicious requests without impacting aviation operations.
<p>Application & API Stability</p> <ul style="list-style-type: none">✘ Flight booking, check-in, and passenger information APIs experienced performance degradation under sustained bot-driven traffic floods.	<p>Application & API Stability</p> <ul style="list-style-type: none">✔ APIs remained stable under peak load with intelligent traffic filtering and adaptive request control.
<p>Bot & Traffic Differentiation</p> <ul style="list-style-type: none">✘ Static defenses could not distinguish between legitimate passengers and sophisticated bot traffic using spoofed identities and rotating IPs.	<p>Bot & Traffic Differentiation</p> <ul style="list-style-type: none">✔ Behavioral AI models accurately identified bots vs genuine users, ensuring only legitimate passenger traffic was processed.

"In aviation, disruption is not measured in downtime—it is measured in passengers affected. Resilience defines operational success."



Trusted by aviation infrastructure providers to ensure uninterrupted operations with AI-native WAAP, real-time DDoS mitigation, and adaptive application protection.



Protect Aviation Systems with AI-Driven Unified WAAP Platform in Minutes