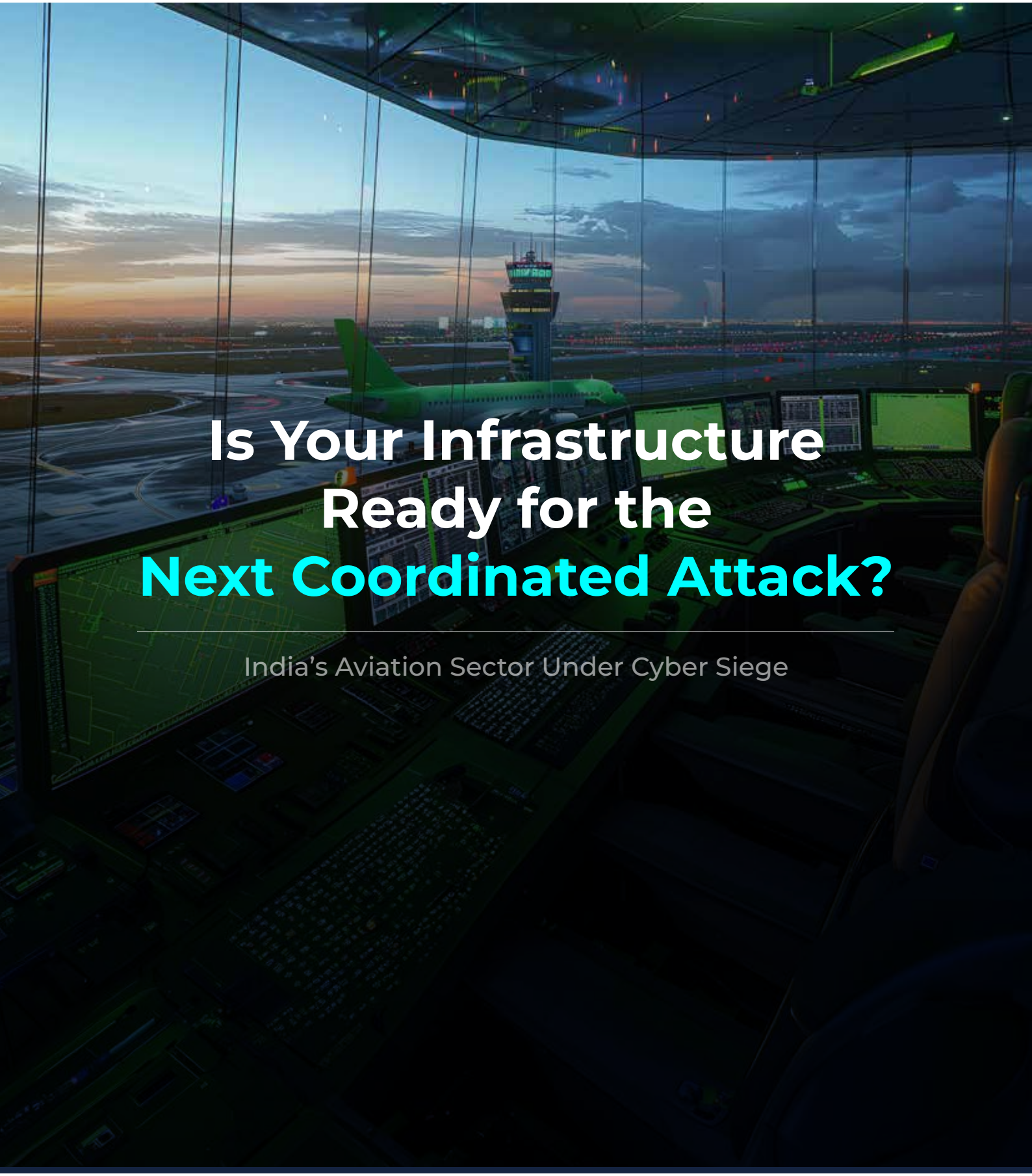
Prophaze
The New Phase of Security

Case Study



Is Your Infrastructure Ready for the Next Coordinated Attack?

India's Aviation Sector Under Cyber Siege

APRIL 2023 AVIATION INDUSTRY | AIRPORT SYSTEMS | CRITICAL INFRASTRUCTURE

A comprehensive study on multi-layered Layer 7 DDoS mitigation in critical aviation infrastructure.

Request demo

The Hidden Crisis Behind India's Airports

While passengers experienced delays and chaos on the surface, a far more dangerous battle was unfolding behind the scenes—within the digital backbone of India's busiest airports.

In April 2023, six of India's busiest airports became the target of a coordinated Layer 3-7 DDoS attack. Unlike traditional traffic floods, this campaign leveraged distributed botnets that bypassed perimeter defenses by mimicking legitimate user behavior.

The challenge was not just the scale—over 50 million requests and traffic peaks reaching 450 Gbps—but the precision. The attackers targeted critical application endpoints used for flight bookings, check-in operations, and real-time data exchange,

> *"Critical infrastructure today isn't just physical—it's deeply digital. And when digital systems fail, the impact is immediate, visible, and global."*
>
> **— Aviation Security Analyst**

IMPACT SNAPSHOT: APRIL

Layer 7 HTTP Floods:
Massive saturation targeting application layers and APIs

IP Rotation & Evasion:
Spoofed identities bypassing traditional WAF defenses

Botnet Orchestration:
Automated large-scale traffic overwhelming systems

API Exploitation:
Targeted disruption of critical operational endpoints

Critical Vulnerabilities Exposed

Application Layer Targeting
Overloading APIs and web applications powering airport operations

Legacy Security Gaps
Static defenses failing against dynamic, evolving threats

Bot-driven Traffic Floods
Massive automated request surges overwhelming systems

Solution: Prophaze WAAP Platform

Defending aviation infrastructure with a **multi-layered, AI-driven security architecture** designed for real-time resilience. Prophaze delivered **continuous protection** through intelligent traffic analysis, adaptive scaling, and automated threat mitigation.

Technical Resilience

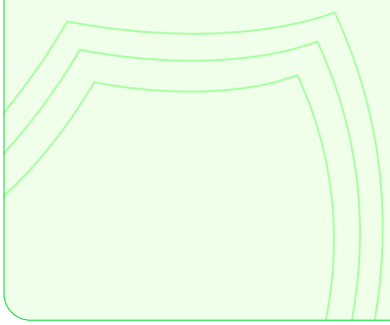
By deploying WAAP architecture via Kubernetes-native environments into the Prophaze security engine, enterprises eliminate critical gaps in their infrastructure.

Legitimate traffic patterns are learned via ML, allowing the system to automatically block the 50M+ malicious requests observed in April 2023 without manual intervention.

STATUS: LIVE PROTECTION

99.99%

UPTIME DURING ATTACK



Core Defense Capabilities

Real-time DDoS Mitigation
Absorbed 450 Gbps attack traffic without latency impact

AI/ML Traffic Intelligence
Behavior-based detection of bots and anomalies

CAPTCHA-less Bot Defense
Advanced filtering without disrupting user experience

Kubernetes-Native Scaling
Auto-scaling infrastructure to handle attack spikes

Centralized WAAP Control
Unified visibility across all airport systems

Custom Rate Limiting
Protection of sensitive APIs from targeted abuse

Geo-Fencing & Proxy Blocking
Preventing malicious traffic from high-risk regions

Results – Zero Disruption, Maximum Protection

Post-attack analysis confirms that Prophaze ensured uninterrupted operations across protected airports.

50M+	0ms	100%	450 Gbps
BLOCKED	DOWNTIME	AVAILABILITY	ABSORBED
Malicious Requests	Seamless Operations	Critical Systems Online	Attack Traffic

Attack Composition

Distribution of attack vectors during the April 2023 peak waves

- Layer 7 HTTP floods
- API endpoint targeting
- Bot-driven traffic spikes
- IP spoofing & evasion tactics

Defence Maturity

- Adaptive bot fingerprinting
- Zero-latency traffic filtering
- Elastic scaling under extreme load
- Intelligent API protection

Strategic Impact

By combining **AI-driven anomaly detection, real-time scaling, and deep API protection,** Prophaze successfully neutralized 100% of the coordinated DDoS attempts without manual intervention. The distributed botnet traffic patterns were automatically identified and mitigated within milliseconds of the initial surge.

Will Your Infrastructure Withstand the Next Attack?

Don't wait for disruption to expose your vulnerabilities.
Join 100+ enterprises securing their critical infrastructure with

Request demo