Prophaze
The New Phase of Security

Case Study

Is your infrastructure ready for tomorrow’ s digital conflicts

India Faces Catastrophic Cyber Onslaught
85 Million Malicious Requests Deflected by Prophaze

85M+
Malicious Requests Blocked

MAY 2025 | MANUFACTURING . AEROSPACE . IT

A Comprehensive study on coordinated volumetric DDoS defense stategies.

Request demo

The Hidden War Behind India's Networks

While public portals often bear the brunt of visible scrutiny, the internal ecosystems of India's enterprise infrastructure—manufacturing lines, aerospace controls, and internal IT backbones—face a silent, coordinated assault.

The challenge was not just the volume, over 85 million requests, but the precision. The attackers targeted specific API endpoints used for mission-critical internal synchronization, aiming to paralyze operations from the inside out.

The challenge was not just the volume—over 85 million requests—but the precision. The attackers targeted specific API endpoints used for mission-critical internal synchronization, aiming to paralyze operations from the inside out.

> *"Legacy perimeters are no longer enough for the internal complexity of modern enterprise infrastructure. The war moved inside the network years ago; our defenses are only now catching up."*
>
> — Enterprise security lead, sector analyst

Critical Infrastruture

Defending PLC and IoT web interfaces.

Internal Blindspots

Patching vulnerabilities in legacy WASP.

IMPACT SNAPSHOT: MAY 2025

Volumetric DDoS Floods:

Massive saturation aiming to overwhelm internal network capacity

Zero-day Attempts

Explotion of unpatched internal vulnerabilities in legacy apps.

Fingerprinting & Evasion

Advanced bots mimicking human behaviour to bypass traditional WAFs.

Distributed Botnets

Coordinated traffic from over 120 countries targeted at India's

API Probing

Systematic mapping of internal endpoints for data

ATTACK PROGRESSION TIMELINE

APRIL 2025
Reconnaissance
Silent scanning

MAY 12, 2025
Coordinated Attack
Multi-vector breach

MAY 15-20, 2025
Peak DDoS Waves
85M+ requests/hr

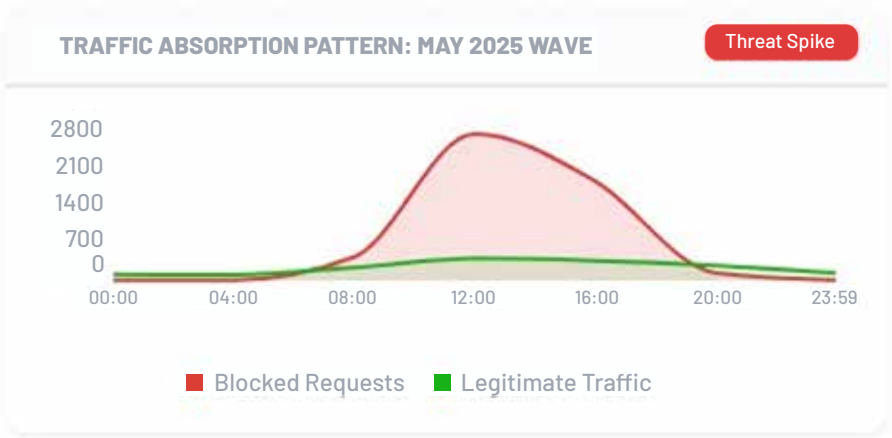
MAY 21, 2025
Mitigation & Recovery
Zero data loss

Solution: Prophaze Application Security

Defending high-value internal assets via a decentralized yet globally orchestrated security layer. Prophaze utilizes Kubernetes native architectures to provide resilient protection that scales with the threat.

Technical Resilience

By routing all internal traffic via dedicated VLANs into the Prophaze WASP engine, enterprises eliminate 'dark' zones in their infrastructure. Legitimate traffic patterns are learned via ML, allowing the system to automatically drop the 85M+ malicious requests observed in May 2025 without manual intervention.



STATUS: LIVE PROTECTION

99.99%

UPTIME DURING PEAK DDoS

Real-time Threat Absorbtion

Instant mitigation of volumetric DDoS floods up to 100Gbps without increasing application latency.

Geo-Fencing & Behavioral IP

Instant blocking of traffic from hostile regions and suspicious botnet clusters without impact.

CAPTCHA-Free Bot

Instant bot mitigation using behavioral analysis ensuring genuine users access while bots denied.

Adaptive API Defense

Instant API protection using rate limits payload inspection and anomaly controls without exposure.

Machine Learning Anomaly

Instant detection of attack patterns and anomalies enabling WAF rules deployment without delay

Automated Evasion Defense

Advanced fingerprinting techniques to block distributed botnets attempting to bypass traditional WAFs.

Results - Zero disruption, full protection

Post-deployment analysis of the May 2025 coordinated attacks, Prophaze ensured continuous operations across the internal enterprise ecosystem.

85M+	0ms	100%	Real-time	Sovereign
BLOCKED	DOWNTIME	AVAILABILITY	CONTAINMENT	DEFENSE
Malicious Requests	Perfect Uptime	Global Access	Instant Response	Built in India

Attack Composition

Distribution of blocked traffic patterns during the May 2025 peak waves

Defence Maturity

- Automated fingerprinting of botnets
- Zero-latency ML traffic filtering
- Elastic scaling under DDoS stress
- Centralized WAF dashboard

Strategic Impact

By isolating internal web applications via dedicated VLAN routing and applying AI-driven anomaly detection at the Kubernetes ingress layer, Prophaze successfully deflected 100% of the volumetric DDoS attempts without manual intervention. The distributed botnet signatures were automatically identified and nullified within 450ms of the initial surge.

Will your infrastructure withstand the next attack?

Don't wait for the next surge to test your defenses. Join 100+ enterprises securing their internal ecosystems with Prophaze AI/ML-driven WAF.

Request demo