Prophaze™
The New Phase of Security

Case Study

Power & Utilities Sector

THREAT ALERT

Ensured Continuous Operations with Real-Time API Protection and Zero Disruption

In 2023, one of India's leading power providers faced escalating cyber threats targeting APIs that manage grid operations, billing, and mobile payments. SQL injection, XSS, and DDoS attacks exposed critical endpoints, putting operational continuity and public trust at risk.

- API Exploitation Attempts
- Injection & DDoS Attacks
- Zero Downtime Achieved

100%
Attack Block Rate
All injection-based threats successfully mitigated

0 sec
Downtime
Grid, billing, and payment systems remained fully operational

Multi-Million
Malicious Requests Blocked
High-volume API attack traffic neutralized

Real-Time
Threat Detection
Zero-day and unknown threats identified instantly

01 / Situation

Government Infrastructure Under Attack

A leading power provider faced increasing cyber threats targeting APIs managing grid operations, billing systems, and mobile payments. These APIs became critical to daily operations but remained exposed to evolving attack patterns.

Under high traffic and attack conditions, systems struggled to maintain performance. Legacy security controls could not adapt to dynamic threats, leaving applications vulnerable to disruption and instability.

API Exposure

Traffic Surges

Injection Attacks

Bot Traffic

DDoS Flooding

⚠ Critical Citizen Services

⚠ Manual Intervention Dependency

⚠ Performance Degradation

02 / Challenge

Inability to Protect API-Driven Infrastructure

Legacy security lacked visibility and enforcement across distributed API environments

High-Volume Automated & DDoS Attacks

Bot-driven traffic and volumetric floods degraded system performance

No Real-Time Threat Mitigation

Delayed detection allowed attackers to exploit vulnerabilities

Exposure to Zero-Day Threats

Unknown exploits bypassed traditional signature-based defenses

Risk of Lateral Movement

Compromised endpoints threatened backend systems and databases

03 / Solution

Prophaze WAAP: AI-Native Protection for Power Infrastructure

Prophaze deployed an intelligent, API-focused security layer ensuring real-time protection, resilience, and operational continuity.

AI-Powered API Security Enforcement

- Positive security model with strict API access control
- Blocks unauthorized and malicious API requests
- Ensures only trusted traffic reaches systems

Zero-Day Threat Detection & Isolation

- Detects unknown attack patterns instantly
- Isolates compromised endpoints to prevent spread
- Protects backend infrastructure from breaches

Complete Threat Visibility

- Centralized dashboard with real-time insights
- Tracks API usage, threats, and anomalies
- Empowers faster security decision-making

04 / Outcome

Operations Stayed Stable. Power Services Continued Without Disruption.

Here’s what changed during and after deployment:

< 7 Days	**Infrastructure Secured** Critical APIs protected under active attack conditions
0 sec	**Zero Downtime** Grid, billing, and payment systems remained fully accessible
100%	**Block Rate** All SQL injection and XSS attempts neutralized
Real-Time	**Visibility** Complete API monitoring and threat intelligence achieved
100%	**Service Continuity** No disruption to consumers or operational workflows

05 / Comparison

What Changed When Prophaze Was in Place

✗ BEFORE PROPHAZE	✓ AFTER PROPHAZE
API Security Posture	API Security Posture
✗ Legacy firewalls and static WAF rules unable to keep pace with evolving API threats including SQL injection, XSS, and DDoS attacks	✓ AI-native WAAP platform delivering real-time protection, blocking injection attacks, and securing APIs across grid, billing, and payment systems
Attack Handling Capability	Attack Handling Capability
✗ No real-time mitigation against application-layer attacks, leaving systems exposed during active exploitation attempts	✓ Instant detection and mitigation of SQL injection, XSS, and DDoS attacks with zero downtime across critical services
Application Stability	Application Stability
✗ Frequent disruptions caused by bot traffic, automated attacks, and resource exhaustion impacting performance	✓ Stable and continuously available systems with intelligent filtering, bot mitigation, and adaptive traffic control

"In critical infrastructure, security is not optional—it's the foundation of uninterrupted service and public trust."

Prophaze™
The New Phase of Security

Trusted by global enterprises, manufacturers, and exporters to maintain uninterrupted operations with AI-driven unified traffic management and failover protection.

Secure Power Infrastructure with Prophaze WAAP Platform