

Prophaze WAAP

Web Application & API Protection

Unified application security with AI-driven detection, runtime protection, and inline enforcement



The Application Security Gap

Securing the Modern Digital Frontier

In the era of rapid digital transformation, the boundaries of the traditional corporate network have dissolved. Applications are no longer monolithic entities behind a firewall; they are distributed microservices communicating across hybrid-cloud environments. This shift has created a massive Application Security Gap.

At the same time, fragmented security tools lack the context and coordination required to protect dynamic, distributed environments.

It is time to move beyond reactive security and embrace proactive, intelligent enforcement.

Prophaze WAAP Platform

Prophaze WAAP consolidates application security into a single platform that combines WAF, API protection, bot mitigation, and Layer 7 DDoS defense with shared intelligence and unified policy enforcement.

The platform operates inline or at the edge, continuously analyzing traffic, learning application behavior, and enforcing protection in real time.

Delivers unified visibility and control across all application traffic, enabling security teams to detect anomalies faster, respond to threats proactively, and maintain consistent policy enforcement across distributed environments.



Market Insight

50%+

Of web traffic is now API-driven

The explosion of microservices and mobile apps has shifted the attack surface. Legacy WAFs are blind to this traffic, leaving your core business logic exposed.

Critical Challenges



Multiple disconnected tools across WAF, API security, bot protection, and DDoS



Signature-based detection unable to identify zero-day and behavioral attacks



API gateways lacking visibility into abuse and business logic misuse



Bot mitigation operating without application context



Layer 7 attacks bypassing traditional volumetric DDoS defenses

Key Capabilities



Unified Web Application and API Protection

- Integrated protection for web applications and APIs across all Layer 7 entry points.
- Single policy framework correlating Web, API, Bot, and DDoS threats while eliminating gaps.



Integrated Bot Mitigation and Abuse Prevention

- Advanced protection against automated threats across applications and APIs in real time.
- Detects credential stuffing, scraping, and abuse while differentiating bots and applying controls.



API Security and Schema Enforcement

- Comprehensive API protection across ecosystems with discovery and schema validation capabilities.
- Detects API abuse, injection attacks, and misconfigurations while covering OWASP API Top 10 risks.



Inline Enforcement and Virtual Patching

- Real-time enforcement of security policies directly within the application traffic flow.
- Blocks malicious requests while applying access controls, rate limits, and virtual patching.



Centralized Visibility and Security Analytics

- Unified visibility across applications, APIs, bots, and threats with continuous monitoring.
- Delivers correlated insights, logs, and analytics for investigation and response.



AI-Driven Threat Detection and Behavioral Analysis

- Adaptive behavioral intelligence across application user interactions.
- Detects zero-day and unknown threats, identifies anomalies, and reduces false positives.



Layer 7 DDoS Protection

- Protection against application-layer attacks across all Layer 7 environments.
- Mitigates low-and-slow and volumetric attacks using rate limiting and traffic shaping.

Key Differentiators

- ✓ Unified WAAP platform across WAF, API, bot, and DDoS protection
- ✓ AI-driven behavioral detection beyond static signatures
- ✓ Shared intelligence across all traffic entry points
- ✓ Inline protection with zero deployment friction
- ✓ Kubernetes-native architecture for modern workloads
- ✓ Centralized policy enforcement across environments




Deployment Architecture Flexibility

Prophaze WAAP is designed for modern, distributed environments, enabling flexible deployment across

- ☑ Cloud-native deployment across AWS, Azure, and GCP
- ☑ Kubernetes-native protection for containerized workloads
- ☑ On-premises deployment for regulated environments
- ☑ Hybrid deployment across multi-cloud infrastructures
- ☑ Edge and CDN integration for early threat mitigation



INTEGRATION ECOSYSTEM

Supports    Google Cloud
Kubernetes, multi-cloud, and edge CDN integration across modern ecosystems.

Security & Business Outcomes

Security Teams

- ✓ Consolidation of multiple security tools into a unified platform
- ✓ Automated mitigation of OWASP Top 10 and zero-day threats
- ✓ Real-time detection and mitigation of application-layer threats
- ✓ Protection against automated attacks and malicious bot activity

Business Teams

- ✓ Regulatory compliance (PCI-DSS, GDPR, HIPAA)
- ✓ Faster and more secure scaling of modern applications and APIs
- ✓ Improved operational efficiency across security teams
- ✓ Reduced risk of downtime and business disruption

Prophaze Leadership



Ready to secure your application future?

Protect web applications and APIs from modern threats with a single, intelligent platform in 15 minutes

[Request a Demo](#) 