Prophaze Web Application Firewall (WAF)

AI-Driven Application-Layer Defense with Behavioral Analysis, Adaptive Rate Limiting, and Real-Time Mitigation

The Modern Web Security Gap

Securing Dynamic, Distributed Applications at Runtime

Web applications today are dynamic, API-driven, and continuously evolving across cloud, Kubernetes, and hybrid environments. As architectures scale, the attack surface grows faster than traditional security controls can keep up.

Legacy WAFs, relying on static rules and signatures, struggle to detect modern threats such as zero-day exploits, automated attacks, and Layer 7 DDoS. This creates a runtime protection gap, leaving applications exposed without real-time context, adaptability, or precise enforcement.

Prophaze WAF Approach

Prophaze WAF delivers a full-lifecycle, AI-driven security architecture designed for modern application environments. By combining behavioral analysis, deep traffic inspection, and adaptive machine learning, Prophaze continuously learns how applications behave and detects anomalies in real time—before threats can impact users or infrastructure.

The platform enables precise, context-aware protection with near-zero false positives, allowing security teams to enforce policies confidently without disrupting user experience or development velocity. It integrates seamlessly into cloud-native, Kubernetes, and hybrid architectures, empowering DevSecOps teams to deploy and scale protection without code changes or operational overhead.

Market Insight

50%+

Of web traffic is encrypted (HTTPS),

limiting visibility for traditional inspection and signature-based detection models

Critical Challenges

- Signature-based WAFs failing against zero-day and unknown attacks
- High false positives disrupting legitimate users and business flows
- Lack of visibility into encrypted and dynamic application traffic
- Bots and automated attacks mimicking real user behavior
- Fragmented protection across cloud, Kubernetes, and on-prem environments
- Manual rule tuning slowing down DevOps and security teams

Key Capabilities

Adaptive Behavioral WAF Engine

- Continuously learns application behavior, including user interactions, API calls, and traffic patterns.
- Detects anomalies and threats without relying on static rules

Zero-Day Attack Prevention

- Identifies and blocks unknown threats before signatures are available.
- Protects against evolving attack techniques in real time

OWASP Top 10 Protection

- Provides comprehensive protection against critical web vulnerabilities including injection, broken authentication, and misconfigurations.
- Ensures compliance with modern security standards.

Advanced Bot & Automation Defense

- Detects and mitigates bots performing scraping, credential stuffing, and abuse.
- Separates human traffic from automated threats using behavioral intelligence.

Layer 7 DDoS Protection

- Mitigates application-layer attacks using adaptive rate limiting and behavioral controls.
- Protects application availability without impacting legitimate users.

Inline Threat Mitigation & Policy Enforcement

- Applies real-time actions including blocking, rate limiting, and challenge mechanisms.
- Ensures threats are stopped instantly at the request level.

Performance-Optimized Security Engine

- Executes intelligent rule processing to minimize latency and overhead.
- Maintains high application performance while enforcing security controls.

Key Differentiators

- Adaptive WAF that auto-learns application behavior
- Near-zero false positives with precise threat detection
- AI-driven zero-day protection without signature dependency
- Performance-optimized engine with minimal latency
- Advanced response-side security controls
- Kubernetes-native architecture for modern workloads
- Unified policy enforcement across environments

Deployment Architecture Flexibility

Prophaze WAF supports flexible deployment models across modern infrastructures:

- Cloud WAF for AWS, Azure, and GCP environments
- Kubernetes-native WAF for containerized workloads
- On-premises WAF for regulated and controlled environments
- Hybrid WAF for unified multi-environment protection
- Inline and edge deployment for real-time traffic inspection

INTEGRATION ECOSYSTEM

Supports aws Azure Google Cloud Kubernetes, multi-cloud, and edge CDN integration acrossmodern ecosystems.

Security & Business Outcomes

Security Teams

- Detect and block threats in real time with high accuracy
- Eliminate false positives and reduce alert fatigue
- Protect against zero-day, bot, and Layer 7 DDoS attacks
- Strengthen application-layer visibility and control
- Enforce adaptive policies across dynamic workloads in real time

Business Teams

- Ensure uninterrupted user experience and application availability
- Accelerate DevSecOps with zero-code deployment
- Reduce operational overhead from manual rule management
- Enable secure scaling across cloud and hybrid environments
- Support compliance (PCI-DSS, HIPAA, SOC 2, GDPR)

Prophaze Leadership

Take Control of Your Application Security

Secure your applications without compromising performance, users, or development speed in **15 minutes**

Request a Demo