Buyer's Guide

Web Application & API Protection WAAP

Selecting a Unified WAAP Platform for Modern Web, API, and Cloud-Native Environments

Modern applications expose far more than web pages. APIs, microservices, bots, and third-party integrations now carry business-critical logic directly over HTTP, making fragmented security controls ineffective and operationally expensive.

This guide helps security, DevSecOps, and platform teams evaluate WAAP platforms that unify WAF, API security, bot mitigation, and Layer-7 DDoS protection without slowing applications or forcing architectural change.

Who This Checklist Is For

This guide is designed for teams that:

- Run API-first, microservices, or Kubernetes-based applications
- Protect public-facing web apps and APIs
- Face bots, abuse, credential stuffing, and Layer-7 attacks
- Manage multiple security tools with overlapping coverage
- Need zero-code, low-ops protection across cloud, hybrid, and on-prem

1. Unified Threat Detection Across Web, API, Bots & DDoS

WAAP should consolidate protection -not create another silo.

- Does the platform protect web apps, APIs, bots, and Layer-7 DDoS within a single engine?
- Are detections correlated across attack types(e.g., bot-driven API abuse or DDoS blended with credential stuffing)?
- Does it go beyond static signatures using behavioral and anomaly-based detection?
- Can it detect zero-day exploits and business logic abuse?
- Does detection improve automatically as traffic patterns evolve?

2. API Discovery, Abuse Detection & Schema Enforcement

APIs are now the primary attack surface, exposing business logic directly to attackers.

- Can the WAAP automatically discover and inventory APIs, including shadow and undocumented endpoints?
- Does it enforce schemas, methods, and parameter validation?
- Can it detect API abuse, scraping, and credential stuffing beyond authentication failures?
- Are API protections applied without modifying gateways or application code?
- Can API threats be correlated with bot and WAF signals?

3. False Positives, User Experience & Conversion Impact

Security must protect revenue—not disrupt it.

- How does the platform reduce false positives in dynamic applications?
- Can it distinguish real users from bots without an intrusive CAPTCHA?
- Are protections applied transparently to legitimate traffic?
- Does it preserve conversion flows like login, search, and checkout?
- How much manual tuning is required to keep applications functional?

4. Bot Mitigation & Application Abuse Defense

Bots now drive fraud, abuse, and account takeover—not just traffic spikes.

- Does the WAAP include native bot detection and mitigation?
- Can it stop credential stuffing, scraping, and automated fraud?
- Does it detect bots that mimic human behavior?
- Are rate controls adaptive and behavior-based, not static thresholds?
- Can teams allowlist and manage good bots and AI agents safely?

Prophaze
The New Phase of Security

5. Layer-7 DDoS Resilience

Layer-7 attacks bypass traditional DDoS defenses and disrupt availability.

- Does the WAAP protect against HTTP floods, low-and-slow attacks, and API surges?
- Can it baseline normal traffic per app, route, and API?
- Are rate limits dynamic and risk-aware?
- Does mitigation occur in-line or at the edge to protect backends?
- Can it absorb sustained attacks without degrading performance?

6. Deployment & Architectural Fit

WAAP should fit your architecture, not force redesigns.

- Can the platform deploy across cloud, Kubernetes, hybrid, and on-prem?
- Is protection Kubernetes-native, not a bolted-on proxy?
- Does it avoid SDKs, agents, or application code changes?
- Can policies be enforced consistently across environments?
- How quickly can new apps and APIs be onboarded?

7. Visibility, Reporting & Operational Control

Unified protection requires unified visibility.

- Is there a single dashboard for WAF, API, bot, and DDoS activity?
- Can teams view attacks by application, endpoint, region, and risk level?
- Are logs enriched for investigation and forensics?
- Does it support compliance reporting ?
- Can security and DevOps collaborate without tool sprawl?

Why Prophaze for WAAP

Prophaze WAAP delivers full-lifecycle Layer-7 protection for modern applications—unifying WAF, API security, bot mitigation, and DDoS defense in one AI-driven platform. Deployed across cloud, Kubernetes, hybrid, or on-prem environments, Prophaze analyzes every request in real time to stop zero-days, bots, and abuse while minimizing false positives and operational overhead.

Prophaze WAAP Delivers

- Unified web, API, bot, and Layer-7 DDoS protection
- AI-driven detection beyond static rules
- Automatic API discovery and abuse prevention
- CAPTCHA-free bot mitigation and credential stuffing defense
- Kubernetes-native, multi-cloud, and on-prem deployment
- Centralized visibility, policy control, and compliance reporting

About Prophaze

Prophaze provides an AI-driven WAAP platform that secures APIs and web applications against modern threats such as zero-day attacks, automated abuse, and Layer-7 floods. The platform delivers inline inspection, behavioral analysis, and adaptive enforcement across cloud, Kubernetes, hybrid, and on-prem environments—without requiring SDKs or application code changes.

With centralized visibility, policy consistency, and 24/7 human-in-the-loop operations to reduce false positives, Prophaze helps teams protect API-driven environments while maintaining performance and operational efficiency.

CHOOSE HOW YOU WANT TO GET STARTED

Live Product Walkthrough
Custom Case Review
Architecture Consultation
30-min session

Schedule Demo
Start Free Trial