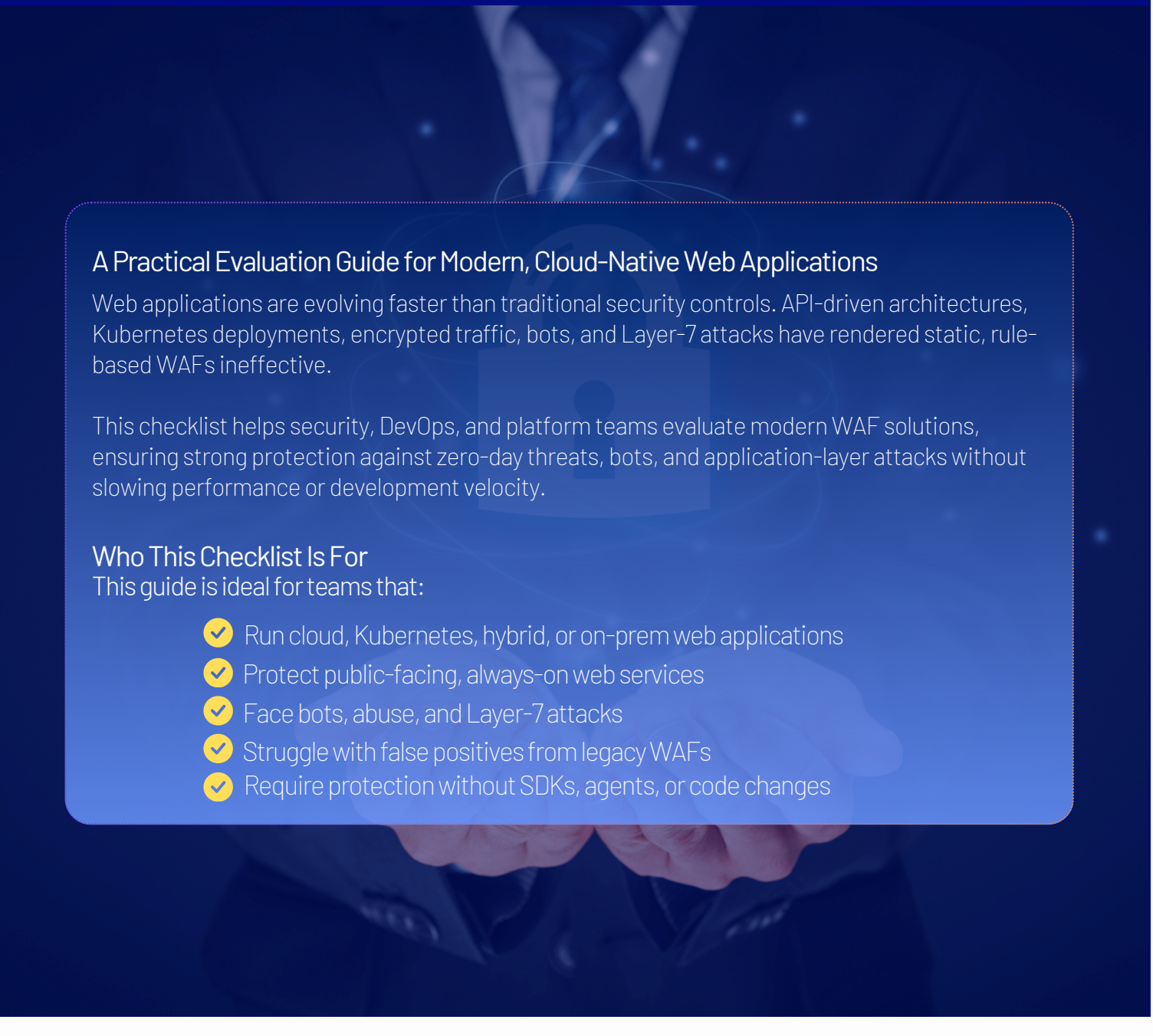
Prophaze™
The New Phase of Security

Buyer's Guide
Web Application Firewall



A Practical Evaluation Guide for Modern, Cloud-Native Web Applications

Web applications are evolving faster than traditional security controls. API-driven architectures, Kubernetes deployments, encrypted traffic, bots, and Layer-7 attacks have rendered static, rule-based WAFs ineffective.

This checklist helps security, DevOps, and platform teams evaluate modern WAF solutions, ensuring strong protection against zero-day threats, bots, and application-layer attacks without slowing performance or development velocity.

Who This Checklist Is For

This guide is ideal for teams that:

- Run cloud, Kubernetes, hybrid, or on-prem web applications
- Protect public-facing, always-on web services
- Face bots, abuse, and Layer-7 attacks
- Struggle with false positives from legacy WAFs
- Require protection without SDKs, agents, or code changes

Prophaze™
The New Phase of Security

1. Threat Detection & Zero-Day Protection

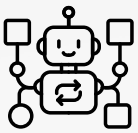
Static rules can't keep up with modern web attacks.

- Can the WAF detect zero-day attacks before signatures exist?
- Does it use adaptive analysis instead of static rule matching?
- Can it detect attacks that blend in with legitimate user traffic?
- Does it protect against OWASP Top 10 threats?
- Does detection improve as traffic patterns evolve?

2. False Positives & User Experience

Blocking attacks should not disrupt real users or applications.

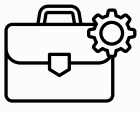
- How does the WAF reduce false positives in dynamic environments?
- Can it distinguish bots from real users without intrusive challenges?
- Are protections applied transparently to legitimate traffic?
- How much manual tuning is required to keep applications working?
- Can policies adapt automatically as application behavior changes?



3. Bot & Layer-7 DDoS Defense

Application-layer abuse is now a leading cause of outages.

- Does the WAF include native bot mitigation?
- Can it detect bots that imitate real user behavior?
- Does it protect against Layer-7 HTTP request floods?
- Are rate controls behavior-based rather than static thresholds?
- Can it absorb sustained attack traffic without exhausting backends?



4. Performance & Developer Experience

Security must protect applications, not slow them down.

- What is the latency impact of inspection and enforcement?
- Is traffic inspected inline or at the edge?
- Does deployment avoid SDKs, agents, or application changes?
- Can security enforce policies without slowing CI/CD pipelines
- Does protection remain stable during traffic spikes?

5. Deployment & Operational Fit

A WAF should adapt to your architecture, not force redesigns.

- Can the WAF protect applications across cloud, Kubernetes, hybrid, and on-prem environments?
- Is the protection model consistent across all environments using a single engine?
- Does it integrate natively with Kubernetes ingress and modern traffic flows?
- Can it fit into existing architectures (CDN, ingress, reverse proxy) without changes to apps or networks?
- How quickly can new applications or services be onboarded?
- How much ongoing effort is required for tuning, policy updates, and operations?

6.Reporting, Compliance & Platform Capabilities

Visibility is essential for fast response and compliance.

- Does the dashboard show real-time attack activity and trends?
- Can threats be viewed by application, region, and attack type?
- Are logs structured for investigation and forensics?
- Does it support compliance reporting (PCI-DSS, HIPAA, etc.)?
- Is the WAF part of a broader application security platform?

Why Prophaze for Web Application Firewall

Prophaze WAF delivers AI-driven, adaptive protection for modern web applications across cloud, Kubernetes, hybrid, and on-prem environments. By analyzing every HTTP request in real time, Prophaze blocks zero-day attacks, bots, and Layer-7 abuse while minimizing false positives and preserving application performance.

Prophaze delivers:

- AI-powered threat detection that adapts in real time
- Zero-day and OWASP Top 10 protection
- Built-in bot and Layer-7 DDoS defense
- Kubernetes-native and multi-cloud deployment
- Unified dashboard for visibility, policy control, and compliance

Prophaze™
The New Phase of Security

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