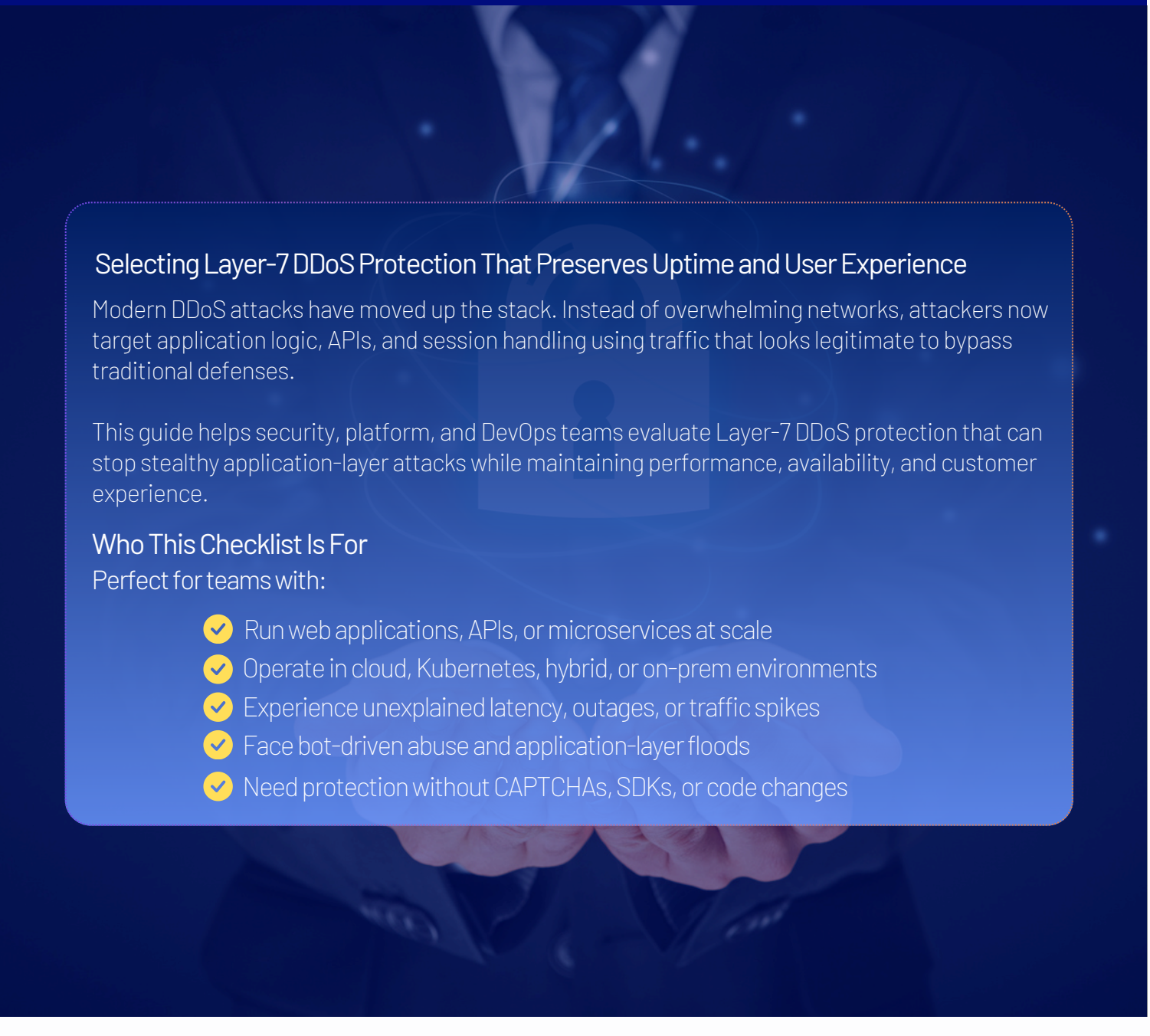
Prophaze™
The New Phase of Security

Buyer's Guide

Layer-7 DDoS Protection



Selecting Layer-7 DDoS Protection That Preserves Uptime and User Experience

Modern DDoS attacks have moved up the stack. Instead of overwhelming networks, attackers now target application logic, APIs, and session handling using traffic that looks legitimate to bypass traditional defenses.

This guide helps security, platform, and DevOps teams evaluate Layer-7 DDoS protection that can stop stealthy application-layer attacks while maintaining performance, availability, and customer experience.

Who This Checklist Is For

Perfect for teams with:

- Run web applications, APIs, or microservices at scale
- Operate in cloud, Kubernetes, hybrid, or on-prem environments
- Experience unexplained latency, outages, or traffic spikes
- Face bot-driven abuse and application-layer floods
- Need protection without CAPTCHAs, SDKs, or code changes

Prophaze™
The New Phase of Security

1. Detecting Modern Layer-7 DDoS Attacks

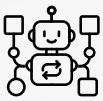
Application-layer DDoS attacks are designed to evade traditional thresholds and signatures.

- Can the solution detect HTTP floods, Slowloris, and low-and-slow attacks?
- Does it identify attacks that mimic normal user behavior?
- Can it distinguish malicious surges from legitimate traffic spikes?
- Does detection adapt as traffic patterns and attack techniques evolve?
- Can it identify abuse targeting specific endpoints, routes, or APIs?

2. Business Impact & Attack Visibility

Layer-7 attacks often go unnoticed, silently driving infrastructure costs, disrupting revenue-critical flows, and causing outages without triggering traditional DDoS alerts.

- Can the platform show which applications, APIs, or routes are under attack?
- Does it highlight the impact on logins, checkouts, search, and other critical flows?
- Can teams see attack trends and escalation in real time?
- Is visibility unified across cloud, Kubernetes, and on-prem environments?
- Does it reduce alert noise while surfacing real risk quickly?



3. Bot-Driven and Blended Attack Defense

Most Layer-7 DDoS campaigns rely on automation, not raw volume.

- Does the solution include a built-in bot and automation detection?
- Can it stop bot-driven API floods and session abuse?
- Does it avoid CAPTCHA and friction for legitimate users?
- Can it handle blended attacks combining bots, APIs, and low-rate floods?
- Are mitigation decisions behavior-based rather than static rate limits?

4. Mitigation Without User Disruption

Stopping attacks should not degrade performance or user experience.

- Are rate limits adaptive and behavior-aware rather than hard-coded?
- Can mitigation be applied per route, method, or endpoint?
- Does enforcement preserve legitimate sessions during attacks?
- Is mitigation automatic, or does it require manual intervention?
- Can the platform sustain prolonged attacks without backend exhaustion?

5. Deployment & Architectural Fit

Layer-7 protection must work where applications actually run.

- Can it deploy across cloud, Kubernetes, hybrid, and on-prem environments
- Is Kubernetes-native enforcement supported at the ingress and service layers
- Does deployment avoid agents, SDKs, or application changes?
- Can mitigation run inline or at the edge with minimal latency?

6. Operational Control & Reporting

Visibility and control are critical during live incidents.

- Is there a single dashboard for attack visibility and mitigation status?
- Can teams investigate incidents with enriched logs and timelines?
- Are geo, ASN, and IP controls available for rapid response?
- Can reports support audits, post-incident reviews, and leadership updates?
- Does the platform integrate with SIEM and incident workflows?

Why Prophaze for Layer-7 DDoS Protection

Prophaze delivers application-aware Layer-7 DDoS protection that stops stealthy floods, low-and-slow attacks, and bot-driven abuse without disrupting legitimate users. By combining behavioral analysis, adaptive rate limiting, and Kubernetes-native enforcement, Prophaze protects web apps and APIs across cloud, hybrid, and on-prem environments.

Prophaze Delivers:

- AI-driven detection of modern Layer-7 DDoS patterns
- Adaptive mitigation that preserves real user sessions
- Built-in bot and API abuse defense
- Kubernetes-native, cloud, and on-prem deployment
- Unified visibility across applications and environments

Prophaze™
The New Phase of Security

About Prophaze

Prophaze is an AI-powered WAAP platform designed to secure modern web applications, APIs, and cloud-native architectures. The platform combines deep traffic inspection, behavioral analytics, and adaptive enforcement to protect against zero-day attacks, bots, and application-layer DDoS without requiring code changes or constant tuning.

Deployed across cloud, Kubernetes, hybrid, and on-prem environments, Prophaze provides unified visibility, real-time mitigation, and operational simplicity for security and DevSecOps teams protecting always-on digital services.

CHOOSE HOW YOU WANT TO GET STARTED

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

Schedule Demo

Start Free Trial