Prophaze™
The New Phase of Security

Buyer's Guide
Bot Protection

An Evaluation Framework for Modern Bot and Automation Defense

Malicious automation now drives a significant share of internet traffic. From credential stuffing and scraping to fraud bots and low-and-slow automation campaigns, attackers exploit web apps and APIs at scale often without triggering traditional security controls.

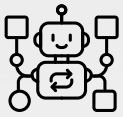
This evaluation framework helps security, fraud, and platform teams assess bot protection solutions that can stop automated abuse in real time without harming user experience, conversion rates, or application performance.

Who This Guide Is For

This guide is ideal for teams that:

- Run revenue-critical web applications and APIs
- Face credential stuffing, scraping, and automated fraud
- See rising infrastructure costs from bot-driven traffic
- Want bot defense without CAPTCHAs, SDKs, or code changes
- Need visibility into automation impacting business metrics

Prophaze™
The New Phase of Security



1. Bot Detection & Automation Intelligence

Modern bots don't behave like obvious attackers—they imitate real users.

- Can the platform detect human-like automation campaigns, not just basic scripts?
- Does it identify credential stuffing attempts across login and API endpoints?
- Can it distinguish between bots and humans using behavioral patterns, rather than static signatures?
- Does detection adapt as bot tactics and tools evolve?
- Can it identify coordinated bot campaigns across sessions and IPs?

2. User Experience & False Positives

Bot protection should stop abuse without blocking customers or breaking flows.

- How does the solution prevent false positives during peak traffic?
- Are mitigations invisible to real users whenever possible?
- Can it protect logins and checkout flows without CAPTCHAs?
- How does it ensure real customers aren't challenged or throttled?
- Does protection adapt automatically as user behavior changes ?

3. Credential Stuffing & Automated Abuse

Account takeover and fraud often start with leaked credentials and automation.

- Can the platform detect large-scale credential stuffing across web and APIs?
- Does it spot low-and-slow login abuse designed to evade rate limits?
- Can it protect password reset, OTP, and authentication endpoints?
- Does it correlate failed logins, retries, and automation patterns in real time?
- Can it stop abuse before fraud and downstream security tools detect damage?

4. Bot Mitigation & Response Controls

Detection alone isn't enough; response must be precise and adaptive.

- What mitigation options are available (rate limits, challenges, blocks, redirects)?
- Can responses be tailored per bot type and business flow?
- Are adaptive controls used instead of static thresholds?
- Can good bots (search engines, partners, monitoring) be safely allowed?
- Does mitigation protect infrastructure from cost-inflating bot traffic?

5. Deployment & Operational Fit

Bot protection must seamlessly integrate with existing architectures.

- Can the platform deploy across cloud, Kubernetes, edge, and on-prem?
- Does it avoid SDKs, agents, or application rewrites?
- Can bots be stopped at the edge before they hit origin infrastructure?
- How quickly can protection go live for new apps and APIs?
- Does deployment introduce any measurable latency?

6. Visibility, Reporting & Business Impact

Bot defense must be measurable not a black box.

- Can teams see bot traffic, automation campaigns, and trends in real time?
- Does reporting show impact on fraud reduction, conversion, and infra costs?
- Can activity be analyzed by endpoint, region, bot type, and attack pattern?
- Are logs available for audits, investigations, and executive reporting?
- Can security, fraud, and business teams share one source of truth?

Why Prophaze for Bot Protection

Prophaze Bot Protection uses AI-driven behavioral analytics and real-time automation intelligence to stop bots that evade traditional controls. From credential stuffing and scraping to fraud bots and large-scale automation campaigns, Prophaze protects web apps and APIs without CAPTCHAs, broken user journeys, or added latency.

Prophaze Delivers:

- Behavioral detection for human-like bots and automation campaigns
- Credential stuffing and account abuse protection
- Adaptive rate limiting and low-friction challenges
- Cloud, Kubernetes, edge, and hybrid deployment
- Unified bot analytics tied to security and business impact

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