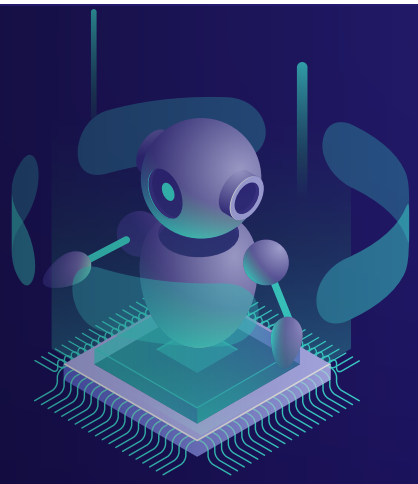
Prophaze Bot Protection

Real-Time Bot Mitigation with Behavioral Intelligence, Intent-Based Classification, and Inline Enforcement



The Bot Threat Landscape

Securing Applications from Malicious Automation

Automated bot traffic now dominates a significant portion of internet activity, directly targeting web applications, APIs, and digital business workflows. From credential stuffing and scraping to fraud automation and resource abuse, bots are no longer simple scripts they mimic human behavior, evade traditional defenses, and operate at scale.

As organizations expand across cloud-native architectures, microservices, and distributed environments, bot attacks increasingly bypass legacy controls such as CAPTCHAs and rate limiting.

Prophaze Bot Protection Approach

Prophaze Bot Protection closes this gap with a runtime-first, AI-driven bot mitigation architecture powered by the BotCry™ Engine. By combining behavioral analytics, intent-based classification, and multi-layered detection, Prophaze identifies and stops bots in real time without impacting legitimate users or introducing friction.

It provides continuous visibility and precise control over automated traffic, enabling security, fraud, and platform teams to detect, prioritize, and mitigate bot threats across web applications and APIs. The platform integrates seamlessly into modern environments including Kubernetes, cloud, APIs, and edge/CDN layers, ensuring protection without code changes, SDKs, or deployment delays.

Market Insight

80%+

Of credential stuffing and account takeover attacks are executed using automated bot frameworks

Critical Challenges

- Malicious bots mimicking human behavior to evade detection
- Credential stuffing and account takeover attacks at scale
- Content scraping impacting revenue, pricing, and intellectual property
- Automated fraud including fake signups, card testing, and checkout abuse
- API endpoint abuse by bots targeting business logic flows
- Ineffective traditional controls (CAPTCHAs, rate limits) causing user friction
- Lack of unified visibility across bot, API, and application traffic

Key Capabilities

Intent-Based Bot Detection & Classification

- Identifies bots based on intent, behavior, and interaction patterns—not just signatures.
- Distinguishes between good bots, malicious automation, and human users with high accuracy.

Advanced Behavioral Fingerprinting

- Analyzes user interactions such as navigation patterns, mouse movements, typing cadence, and session behavior.
- Detects human-like bots attempting to mimic legitimate users

Protection Against Automated Fraud & Abuse

- Prevents credential stuffing, account takeovers, fake registrations, scraping, and checkout abuse.
- Stops bots before they impact revenue or user trust.

Centralized Bot Visibility & Analytics

- Provides a unified dashboard to monitor bot activity, attack trends, and traffic distribution.
- Enables deep investigation, reporting, and optimization of defenses.

Adaptive Rate Limiting & Throttling

- Dynamically controls high-frequency bot traffic based on behavior and risk.
- Mitigates volumetric and low-and-slow bot attacks in real time.

API Bot Protection & Anomaly Detection

- Monitors API traffic patterns and detects abnormal bot activity targeting endpoints.
- Protects both public and shadow APIs from automated exploitation.

Inline Mitigation & Real-Time Enforcement

- Enforces policies directly in the traffic path with immediate response actions.
- Blocks, redirects, challenges, or throttles bot traffic without impacting application performance.

Key Differentiators

- Intent-based bot classification beyond traditional methods
- Advanced behavioral fingerprinting for human-like bots
- Invisible, low-friction challenges (no CAPTCHA dependency)
- Real-time inline mitigation with zero code changes
- API-aware bot protection across all endpoints
- Kubernetes-native architecture for modern applications
- Unified visibility across bot, API, and application traffic

Deployment Architecture Flexibility

Prophaze Bot Protection supports flexible deployment models to align with enterprise environments:

- Cloud deployment across AWS, Azure, and GCP On-premises deployment for controlled infrastructures
- Hybrid deployment across distributed environments
- Kubernetes-native integration for microservices architectures
- Inline proxy deployment with zero application changes
- Edge/CDN integration to stop bots before reaching origin

INTEGRATION ECOSYSTEM

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

Security & Business Outcomes

Security Teams

- Eliminate bot-driven threats and automated abuse
- Prevent account takeover and credential based attacks
- Detect and stop bots in real time with high accuracy
- Reduce false positives and improve user experience
- Gain continuous visibility and control over automated traffic

Business Teams

- Protect revenue from scraping and fraud automation
- Maintain seamless user experience without friction
- Reduce infrastructure costs from bot traffic overload
- Enable secure scaling of digital platforms and APIs
- Support compliance requirements (PCI-DSS, GDPR, HIPAA)

Prophaze Leadership

GARTNER Peer Insights STRONG PERFORMER Voice of the Customer 2025

Vendor in GARTNER Market Guide WAAP 2025

High Performer FALL 2024

Overall Leader 2024

Mentioned in GARTNER Market Guide API Security 2024

Innovation Leader 2022

Take Control of Your Bot Traffic

Secure your applications with intelligent bot detection, real-time mitigation, and seamless user experience in 15 minutes

Request a Demo