Prophaze™
The New Phase of Security

PRODUCT DATA SHEET

Prophaze DDoS Protection

AI-Driven Layer 7 DDoS Defense with Behavioral Analysis and Real-Time Mitigation

The DDoS Protection Gap

Securing the Modern Application Layer

Modern DDoS attacks have evolved beyond volumetric floods to target the application layer with precision. Attackers increasingly use low-and-slow techniques, bot-driven requests, and API abuse patterns that mimic legitimate traffic, making traditional network-layer defenses ineffective.

As applications scale across microservices, Kubernetes, and multi-cloud environments, maintaining availability requires intelligent, application-aware protection.

Prophaze DDoS Protection Approach

Prophaze delivers an application-aware, runtime DDoS protection architecture that combines traffic baselining, behavioral analysis, and inline mitigation. The platform continuously learns normal traffic patterns and enforces adaptive controls to stop attacks in real time while preserving user experience and uptime.

It delivers unified visibility and control across applications, APIs, and microservices, enabling security teams to detect attacks faster, respond proactively, and maintain uninterrupted service availability.

It also integrates seamlessly with cloud, on-premises, and hybrid environments, as well as Kubernetes and edge/CDN infrastructures, enabling consistent protection without code changes or operational friction. This ensures applications, APIs, and microservices remain resilient and available even under sophisticated Layer 7 DDoS attacks.

Market Insight

200M+

malicious requests per hour
now hit enterprises

With Layer 7 DDoS attacks silently draining resources. Traditional network defenses can't detect bot-driven, behavioral traffic, putting uptime, data, and revenue at risk.

Critical Challenges

- Application-layer floods that mimic legitimate user behavior
- Low-and-slow attacks that silently exhaust server resources
- Bot-driven API requests targeting backend logic and services
- Microservices and Kubernetes architectures expanding attack surfaces
- Traditional defenses unable to detect context-aware and behavioral attacks

Key Capabilities

Intelligent Layer 7 DDoS Detection

- Detects application-layer attacks that bypass traditional defenses.
- Identifies HTTP floods, Slowloris, and low-rate DDoS patterns using multi-layer behavioral analysis.

Behavioral Traffic Baselining and Anomaly Detection

- Learns normal traffic patterns per endpoint, route, and service.
- Detects abnormal spikes, bursts, and distributed attack patterns in real time.

Adaptive Rate Limiting and Traffic Control

- Applies dynamic rate limiting and granular traffic controls by IP, user, endpoint, and request type.
- Prevents resource exhaustion while preserving legitimate user experience.

Bot and API Abuse Mitigation

- Stops automated attacks targeting applications and APIs.
- Detects credential stuffing, scraping, and bot-driven floods while filtering malicious automation without CAPTCHA friction.

Deep Request Inspection and Protocol Protection

- Analyzes HTTP/HTTPS headers, payloads, and request structures to detect malicious activity.
- Supports TCP, UDP, ICMP, DNS, and application-layer protocols while identifying injection attempts and anomalies.

Inline Mitigation and Real-Time Enforcement

- Blocks malicious requests directly in the traffic path in real time.
- Applies rate limiting, filtering, and access control policies to protect backend systems while ensuring uninterrupted access for legitimate users.

Centralized Visibility and Attack Analytics

- Provides unified visibility into DDoS activity and mitigation.
- Delivers real-time monitoring, visual insights, detailed logs, and compliance reporting for investigation and response.

Key Differentiators

- Intelligent detection distinguishing real users from attack traffic
- Multi-layer behavioral analysis for precise mitigation
- Application-layer (Layer 7) focused DDoS protection
- Inline mitigation with zero deployment friction
- Context-aware protection across web, API, and microservices
- Kubernetes-native architecture for modern workloads

Deployment Architecture Flexibility

Prophaze DDoS Protection is designed for flexible deployment across environments:

- Cloud-native deployment across AWS, Azure, and GCP
- On-premises deployment for full control and compliance
- Kubernetes-native integration for microservices environments
- Hybrid deployment across distributed infrastructures
- Edge and CDN integration for early attack mitigation

INTEGRATION ECOSYSTEM

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

Security & Business Outcomes

Security Teams

- Ensure uninterrupted application availability during attacks
- Detect and mitigate Layer 7 DDoS threats in real time
- Prevent downtime caused by malicious traffic
- Protect APIs and backend services from abuse and overload

Business Teams

- Enable secure scaling of application infrastructure
- Reduce operational complexity and manual intervention
- Faster and safer deployment of modern applications
- Improved operational efficiency for security teams

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 kuppingercole Overall Leader 2024

Mentioned in GARTNER Market Guide API Security 2024

INNOVATION LEADER kuppingercole Innovation Leader 2022

Stop Layer 7 DDoS Attacks Before They Impact Availability

Protect web applications, APIs, and microservices with intelligent, real-time DDoS defense **15 minutes.**

Request a Demo