How Prophaze — Protects Your Apps

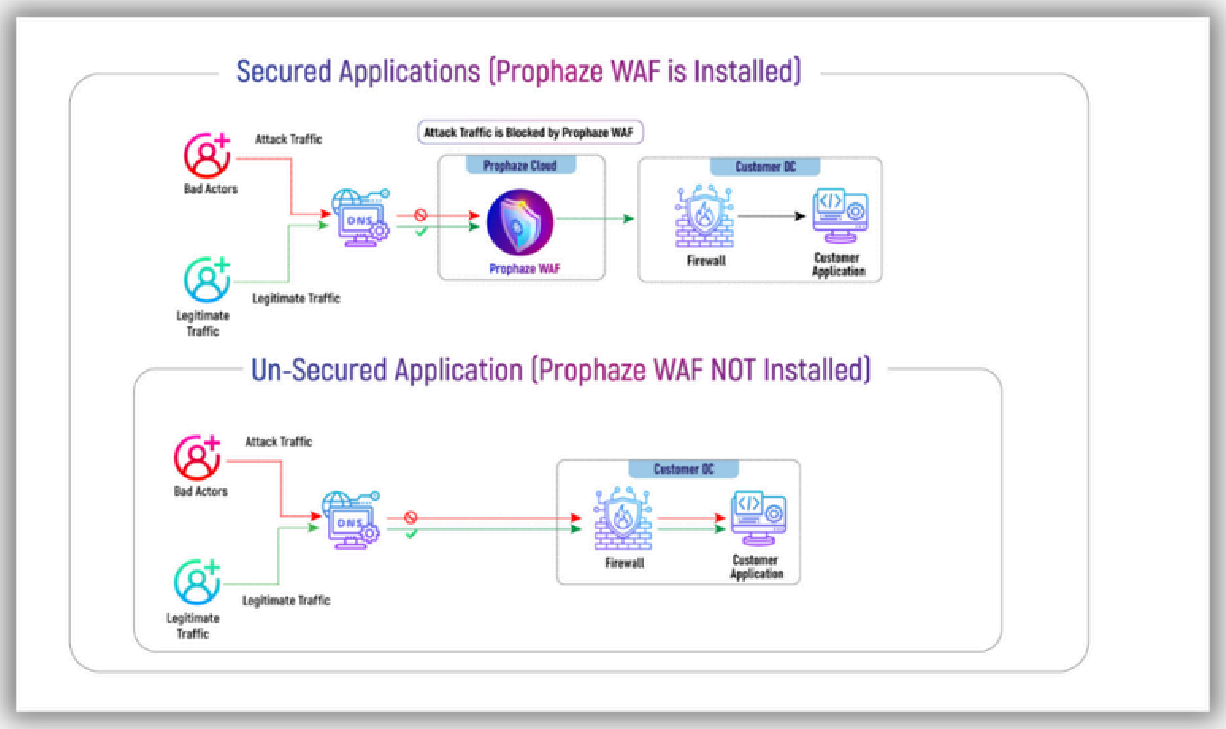
Prophaze™

The New Phase of Security

How It Works

Prophaze is a cloud-native Web Application and API Protection (WAAP) platform that sits in front of your web applications, APIs, and microservices, inspecting every request before it reaches your infrastructure. It combines a powerful WAF, AI-driven detection, and Layer 7 DDoS protection to stop attacks without slowing down your apps. Deployed in minutes, Prophaze shields everything from a single website to applications deployed across any cloud environment.

Image 1: High-level architecture

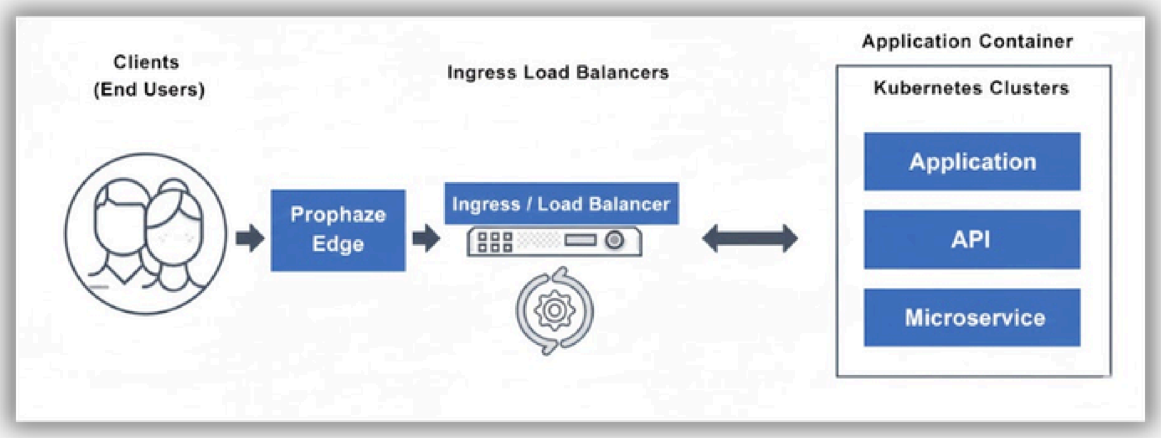


How Traffic Moves Through Prophaze

Request Enters Prophaze Edge

Incoming HTTP/HTTPS traffic is routed through Prophaze using DNS, so every request is inspected at the edge before it touches your origin. Prophaze sits in front of cloud load balancers or K8s ingress, filtering all traffic destined for your web and API services.

Image 2: Flow diagram showing clients → Prophaze edge → load balancer / ingress → application.



Inspection and Decision

At the edge, Prophaze applies a layered inspection pipeline that combines rule sets, signatures, anomaly scores, and AI/ML models. Payloads are scanned for malicious patterns, behavior is compared against known threat profiles, and each request is evaluated against security policies to allow, block, challenge, or rate-limit.

Response Back to User

Legitimate requests are forwarded to your applications with minimal latency, while malicious or suspicious traffic is blocked or challenged, and detailed logs are generated for analysis. This ensures users experience fast, reliable applications while attacks are silently handled in the background.

Inside the Prophaze Protection Engine

WAF & OWASP Top 10 Engine

Prophaze's web application firewall inspects every request to detect and block common and advanced vulnerabilities, including SQL injection, cross-site scripting, remote code execution, and more. Built-in rule sets and virtual patching help protect against OWASP Top 10 risks without requiring code changes.

API Security & Schema Validation

Prophaze tracks and protects your Web APIs by scanning payloads and enforcing expected structures. It uses multiple detection algorithms to distinguish legitimate API calls from malicious ones, ensuring that only valid, well-formed requests reach your services.

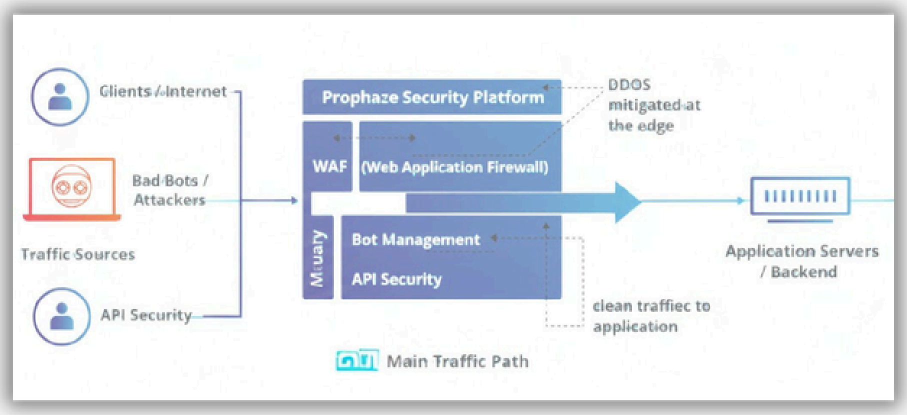
Bot & Abuse Protection

By analyzing behavior and traffic patterns, Prophaze can differentiate good bots from bad ones and block abusive automation, scraping, and brute-force attempts. Rate limiting and fingerprinting techniques keep harmful traffic out while allowing legitimate users and trusted services to continue working.

DDoS & Availability Controls

At Layer 7, Prophaze protects applications from distributed denial-of-service attacks launched through malicious bot networks. It absorbs and filters large volumes of requests so that floods of traffic do not overwhelm your servers, maintaining availability and responsiveness.

Image 3: Security engines block diagram (WAF, API, Bots, DDoS) around the main traffic path.


Glients / Internet
Bad Bots / Attackers
Traffic Sources
API Security
Prophaze Security Platform
WAF
(Web Application Firewall)
Mюary
Bot Management
API Security
DDOS mitigated at the edge
clean traffiec to application
Application Servers / Backend
Main Traffic Path

Cloud-Native Security, Any Environment

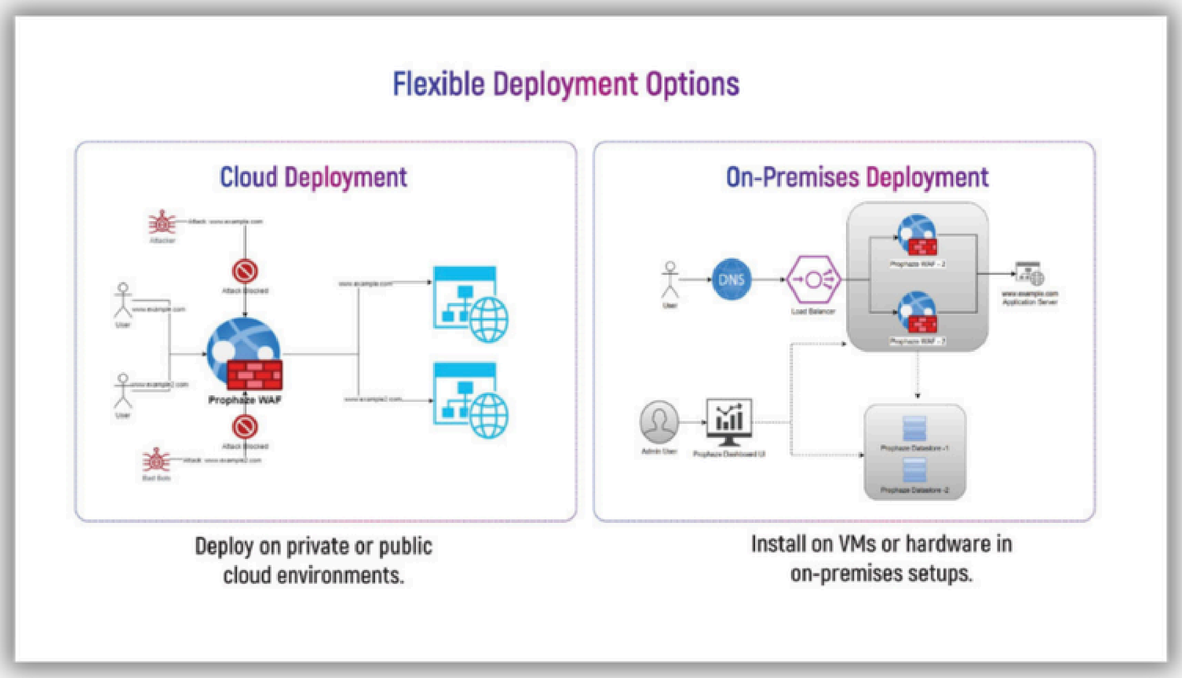
Supported Environments

Prophaze WAF runs seamlessly across public clouds such as AWS, Microsoft Azure, Google Cloud Platform, and DigitalOcean, as well as private cloud and Kubernetes distributions . It is built to protect workloads in containers, VMs, and on-prem environments, supporting hybrid and multi-cloud setups.

Typical Deployment Patterns

You can deploy Prophaze as a reverse proxy in front of your applications, as a Kubernetes ingress controller (KubeWAF) alongside your other components, or as an inline gateway working with your existing load balancers. This flexibility lets you integrate protection with minimal changes to your existing architecture.

Image 4: Multi-cloud / hybrid diagram with Prophaze in front of multiple clouds and a data center.



Flexible Deployment Options

Cloud Deployment

Deploy on private or public cloud environments.

On-Premises Deployment

Install on VMs or hardware in on-premises setups.

How Prophaze Integrates with Your Stack

SIEM & Logging

Prophaze can stream detailed security events and logs to your SIEM and observability tools using formats like JSON or syslog, enabling incident correlation and centralized monitoring. This helps security teams investigate attacks quickly and align WAF data with other telemetry.

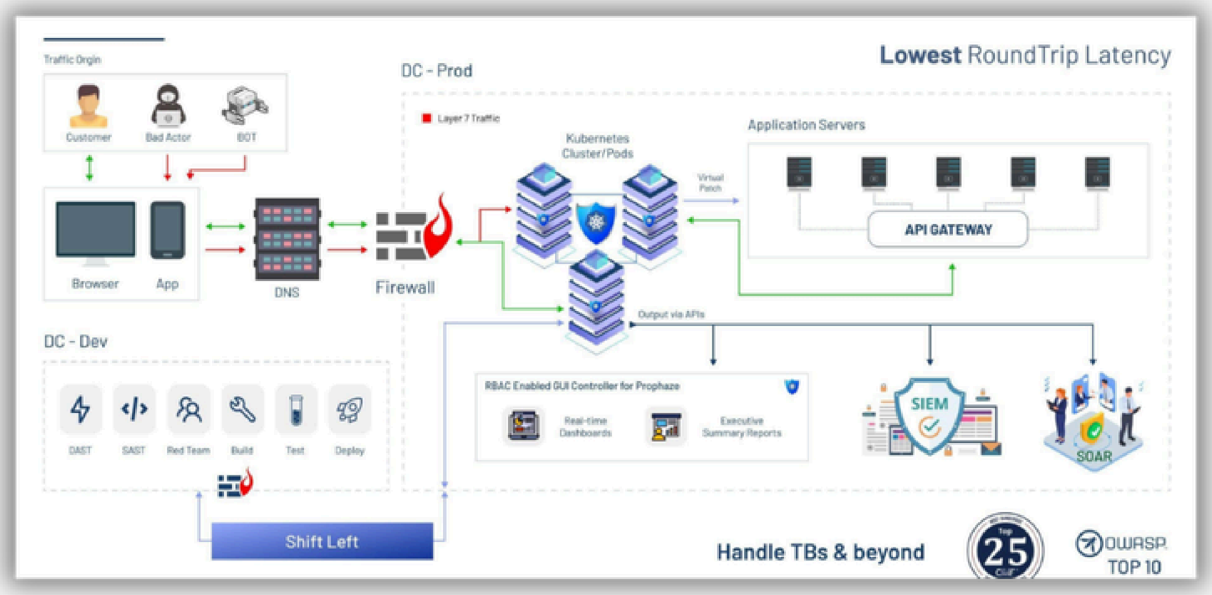
DevSecOps & CI/CD

Using APIs and configuration-as-code patterns, Prophaze can be integrated into CI/CD pipelines so that new applications and APIs are onboarded with consistent security policies from day one. Automated policy updates help keep pace with fast-moving deployments and version changes.

Alerting & Collaboration

Prophaze can send alerts and notifications to collaboration tools like email or chat systems so teams can respond quickly to incidents. Webhooks and integrations ensure the right people are notified when critical thresholds or attack patterns are detected.

Image 5: Integration diagram showing Prophaze sending logs to SIEM and alerts to collaboration tools.



See Everything & Control Everything

Central Dashboard

A central management console provides a single view of your protected websites and APIs, showing live traffic, detected attacks, and overall health trends. This gives security and operations teams a shared, real-time understanding of what is happening across the environment.

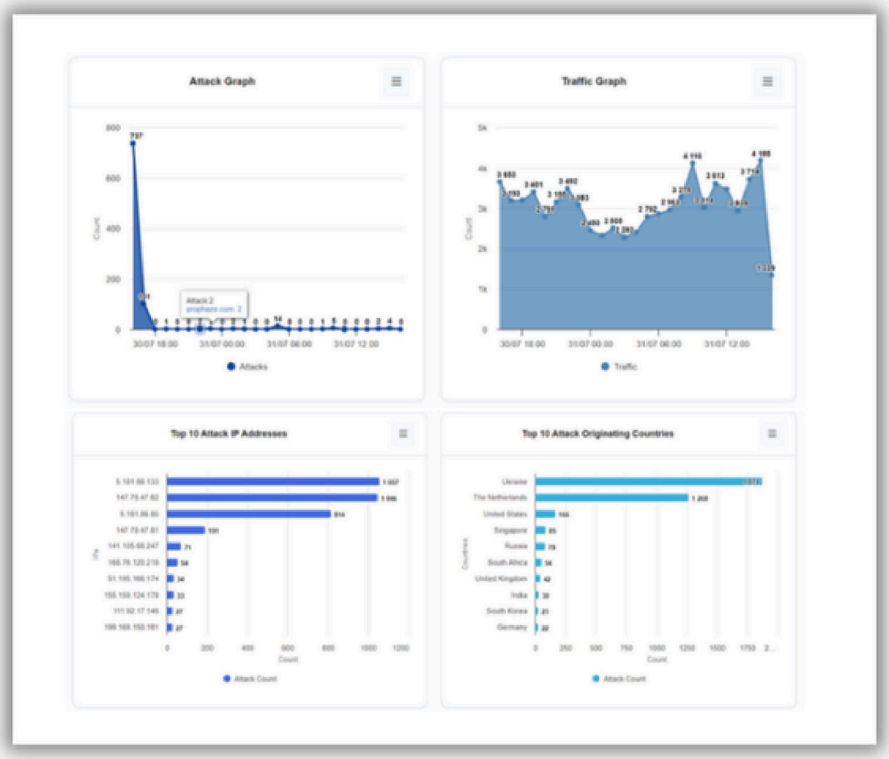
Policy Management

From the dashboard, you can manage global and application-specific policies, including rule sets, access controls, and virtual patches. Fine-grained configuration allows you to tighten security where needed while minimizing false positives.

Reporting & Compliance

Prophaze can generate reports that summarize attack activity, policy actions, and traffic patterns to support audits, SLAs, and regulatory needs such as PCI-DSS, HIPAA, or GDPR. These insights help demonstrate the effectiveness of your web and API protection strategy.

Image 6: Dashboard screenshot or mock showing traffic graphs, attack types, and top targeted endpoints.



Operations & Shared Responsibilities

Prophaze Responsibilities

Prophaze maintains the underlying WAF platform, updates signatures and rule sets, and tunes AI models to stay ahead of emerging threats. When delivered as a managed service, Prophaze's security engineers also help monitor attacks and adjust protections as your environment evolves.

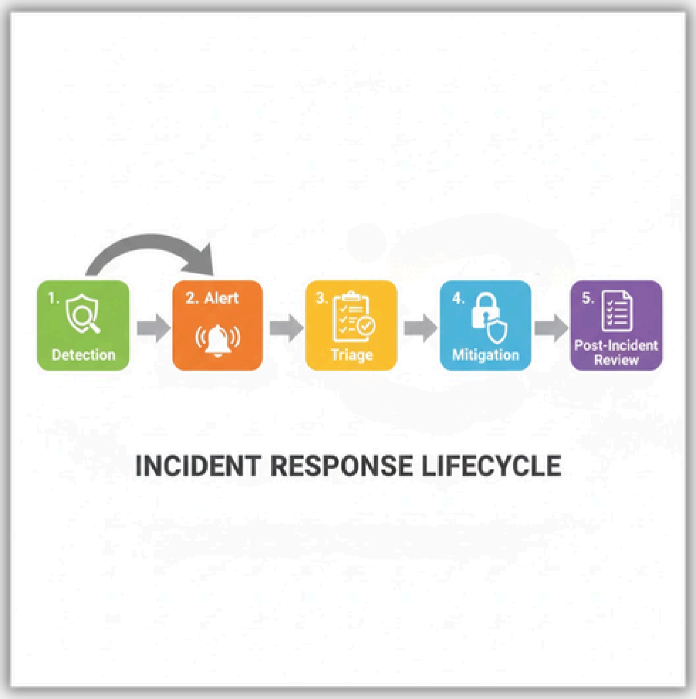
Customer Responsibilities

Your team provides context about applications and APIs, notifies Prophaze of major changes or new deployments, and reviews key alerts or recommended policy updates. This collaboration ensures protections align with your business logic and user experience.

Incident Workflow

When an attack is detected, Prophaze identifies the pattern, raises alerts, and applies mitigation such as blocking or rate limiting in real time. After the incident is contained, logs and insights support post-incident reviews, so policies can be refined and future risk reduced.

Image 7: Lifecycle flow chart: Detection → Alert → Triage → Mitigation → Post-incident review.



Intelligent Protection in Action

AI-Based WAF

Prophaze uses Artificial Intelligence–based engines to inspect every request, categorize it by its threat score, and decide how that traffic should be handled. The platform continuously monitors, tests, and detects malicious behavior while enforcing access controls and authentication safeguards against cyber threats.

Payload Scanning

As a new-generation web application firewall, Prophaze intelligently tracks malicious requests targeting your web APIs and application endpoints. It uses multiple attack detection algorithms to analyze all incoming traffic and ensures only legitimate requests are passed through to your host servers and microservices.

Layer 7 DDoS Protection

Prophaze protects your applications from application-layer (Layer 7) DDoS attacks generated by malicious bot networks and distributed sources. By analyzing request patterns, behavior, and volumes, it detects floods designed to overwhelm your apps and blocks them before they impact availability.

Getting Started

See how Prophaze inspects and protects your sites & APIs with real traffic.

15 Days Free Trial

Book a live demo to explore Prophaze with security experts.

Schedule Demo

Prophaze™

The New Phase of Security

Prophaze Technologies Pvt. Ltd. | Email: security@prophaze.com

Contact: India: +91 7994 008 420 | USA: +1 831 217 6365

OVERALL LEADER KuppingerCole Overall Leader 2024

Vendor in GARTNER Market Guide WAAP 2025

GARTNER Peer Insights STRONG PERFORMER Voice of the Customer 2025

Mentioned in GARTNER Market Guide API Security 2024

G2 HIGH PERFORMER FALL 2024