Prophaze™
The New Phase of Security

PRODUCT DATA SHEET

Prophaze For Kubernetes WAAP Platform (KWAAP)

Kubernetes-Native Web Application and API Protection for Cloud-Native Microservices and Internal Cluster Traffic

The Kubernetes API Security Blind Spot

Securing East-West Traffic Inside Kubernetes

Kubernetes clusters expose hundreds of internal APIs across namespaces, nodes, and microservices. Unlike traditional environments, most cluster communications flow east-west service-to-service, pod-to-pod, and cross-namespace operating entirely outside the reach of perimeter inspection.

These conditions create a structural security gap where internal traffic bypasses Layer 7 analysis, shadow APIs go undiscovered, and behavioral anomalies in authenticated requests remain undetected, leaving cloud-native environments without consistent runtime protection.

Prophaze KWAAP Approach

Prophaze KWAAP delivers a Kubernetes-native, runtime-first security architecture that embeds Layer 7 intelligence directly into cluster communications, providing continuous inspection across ingress, east-west service traffic, cross-namespace calls, and internal API activity. It combines behavioral baselining, continuous API discovery, and inline threat mitigation to detect and stop attacks in real time without impacting performance, integrating seamlessly with ingress controllers, sidecar deployments, and daemonset node agents across multi-cluster, cloud, on-premises, and hybrid Kubernetes environments without code changes or operational overhead.

Market Insight

85%

Global organizations are now running containerized applications in production" a reality Gartner predicted as far back as 2020, making Kubernetes-native web application and API protection an urgent operational necessity.

Critical Challenges

- East-west traffic operating outside perimeter WAF visibility
- Internal APIs exposed to BOLA, token replay, and privilege escalation
- Shadow and undocumented APIs accumulating across microservices
- Lateral movement between services going undetected at runtime
- Gradual API-driven data exfiltration bypassing volume-based controls
- Fragmented security tools across WAF, API gateway, and cluster protection

Key Capabilities

Adaptive Behavioral WAF Engine

- Continuously learns Kubernetes application behavior across ingress, microservices, APIs, and east-west traffic patterns.
- Detects anomalies and threats in real time without relying on static rules or signatures.

East-West Runtime Inspection

- Performs deep Layer 7 payload inspection across internal service-to-service and cross-namespace communications.
- Detects lateral movement, cross-namespace traversal, and boundary violations invisible to perimeter controls.

API-Driven Data Exfiltration Detection

- Monitors object enumeration patterns, retrieval volumes, and cross-service access behavior across internal APIs.
- Identifies gradual exfiltration attempts that remain below infrastructure-level thresholds.

Bot and Automation Detection

- Applies AI-driven behavioral analysis to identify malicious automation targeting internal or exposed APIs.
- Detects credential abuse, scraping, and distributed attack patterns across ingress and east-west traffic.

Layer 7 DDoS Protection

- Mitigates volumetric and application-layer denial-of-service attacks across ingress and internal cluster communications.
- Applies real-time rate limiting and adaptive enforcement with minimal operational overhead.

Continuous API Discovery and Schema Enforcement

- Automatically enumerates REST, GraphQL, and gRPC APIs, including shadow and undocumented endpoints.
- Validates requests against published OpenAPI contracts and blocks undocumented parameter injection and mass assignment attempts.

Identity-Aware Request Analysis

- Detects token replay, service account abuse, and anomalous identity behavior even when credentials are syntactically valid.
- Builds per-service behavioral profiles that flag deviations from established access relationships.

Key Differentiators

- Kubernetes-native WAAP with fast, Helm-based deployment
- Full east-west runtime inspection with no mandatory sidecar injection
- AI-driven detection for behavioral anomalies, BOLA, and token abuse
- Continuous API discovery including shadow and undocumented endpoints
- Unified WAF, API security, bot mitigation, and L7 DDoS in one platform
- Centralized policy enforcement across multi-cluster environments

Deployment Architecture Flexibility

Prophaze KWAAP supports flexible deployment models to align with Kubernetes and enterprise infrastructure requirements.

- Ingress controller integration for north-south Layer 7 inspection at the cluster boundary
- Sidecar-based deployment for per-service east-west inspection without application code changes
- Daemonset node-level coverage providing complete traffic visibility across all pods on each node
- Hybrid and multi-cluster management across EKS, AKS, GKE, and on-premises environments

INTEGRATION ECOSYSTEM

Supports NGINX, Traefik, HAProxy, and ingress controllers across modern Kubernetes deployments

Security & Business Outcomes

For Security Teams

- Eliminate east-west traffic blind spots with runtime Layer 7 inspection
- Detect and mitigate API-layer threats, lateral movement, and token abuse in real time
- Prevent data exfiltration and unauthorized object access
- Improve security posture without impacting application performance

For Business Teams

- Enable secure scaling of cloud-native microservices and APIs
- Regulatory compliance (PCI-DSS, GDPR, HIPAA)
- Consolidate WAF, API security, bot, and DDoS tools into a single platform
- Reduced breach dwell time and total cost of security operations

Prophaze Leadership

Secure What Perimeter Tools Can't See

Protect east-west traffic, internal APIs, and microservice communications with runtime intelligence built for Kubernetes.

Request a Demo