Prophaze API Security

Runtime API Protection with Continuous Discovery, Behavioral Intelligence, and Inline Enforcement

The API Security Gap

Securing the Modern API Ecosystem

APIs have become the **primary control plane of modern applications,** directly exposing business logic, sensitive data, and critical services. As organizations scale across microservices, Kubernetes, and multi-cloud environments, API ecosystems grow faster than traditional security models can govern.

This shift has created **a runtime security gap**—where APIs are active, exposed, and interacting in production environments without sufficient visibility, context, or enforcement.

Prophaze API Security Approach

Prophaze API Security addresses this gap by delivering a runtime-first security architecture that combines continuous API discovery, behavioral intelligence, and inline mitigation, enabling organizations to detect, prioritize, and stop threats in real time without impacting development velocity.

Delivers unified visibility and control across all APIs, enabling security teams to detect anomalies faster, respond proactively, and maintain consistent policy enforcement across distributed environments.

It also integrates seamlessly with CI/CD pipelines, gateways, proxies, and Kubernetes environments, enabling DevSecOps and platform teams to secure APIs without code changes or deployment friction. This ensures consistent protection across cloud, on-premises, and hybrid infrastructures while supporting rapid application scaling.

Market Insight

70%+

East-west traffic (Kubernetes) is largely unmonitored.

30–50%

Of APIs remain undocumented and unprotected

Critical Challenges

- Shadow and zombie APIs operating without visibility
- Business logic flows exploited without triggering signature-based controls
- API schema drift and misconfigurations introducing silent risks
- Credential abuse and automation attacks bypassing traditional controls

Key Capabilities

Continuous API Discovery, Classification & Risk Scoring

- Continuously discovers and inventories all APIs, including known, unknown, and shadow APIs.
- Classifies APIs based on sensitivity and exposure while tracking changes, versions, and access patterns.

Behavioral Threat Detection and API Abuse Protection

- Applies adaptive behavioral analysis to detect anomalies and threats bypassing traditional security controls.
- Identifies credential abuse, automated attacks, and low-frequency or distributed threats.

Protection Against Business Logic Abuse

- Detects and prevents misuse of legitimate API workflows and abnormal API call sequences.
- Monitors user and session behavior to prevent scraping, automation, and data harvesting.

Protection Against OWASP API Security Risks

- Provides protection aligned with the OWASP API Security Top 10.
- Covers BOLA, broken authentication, injection attacks, and security misconfigurations.

Inline Threat Mitigation and Virtual Patching

- enforces security policies directly in the API traffic path in real time.
- Blocks malicious requests, applies rate limiting, and enables virtual patching without code changes.

API Visibility, Monitoring, and Analytics

- Provides centralized visibility into API activity, usage patterns, and performance.
- Identifies high-risk endpoints and delivers actionable insights for investigation and response.

Threat Intelligence and Automated Response

- Leverages real-time threat intelligence to proactively detect emerging API attacks and malicious actors.
- Automates responses to contain threats quickly, minimizing manual investigation and operational overhead.

Key Differentiators

- Continuous API discovery with real-time visibility
- Behavioral analysis for advanced threat detection
- Protection against business logic abuse
- Inline enforcement with no code changes required
- Kubernetes-native architecture for modern workloads
- Unified policy enforcement across environments

Deployment Architecture Flexibility

Prophaze API Security supports flexible deployment models to align with enterprise requirements.

- Cloud deployment across major cloud platforms
- On-premises deployment for controlled environments
- Hybrid deployment across distributed infrastructures
- Kubernetes-native integration for microservices environments
- Integration with gateways, proxies, and edge infrastructure

INTEGRATION ECOSYSTEM

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

Security & Business Outcomes

Security Outcomes

- Reduce API exposure and eliminate blind spots
- Detect and mitigate security threats in real time
- Prevent data loss and unauthorized API abuse
- Improve security posture without impacting development

Business Outcomes

- Enable secure scaling of API-driven applications
- Regulatory compliance (PCI-DSS, GDPR, HIPAA)
- Faster and safer deployment of modern applications
- Reduced risk of downtime and business disruption

Prophaze Leadership

Take Control of Your API Security

Secure your APIs with real-time visibility, intelligent threat detection, and seamless enforcement in 15 minutes

Request a Demo