Revolutionizing Application Security

# Prophaze™

The New Phase of Security

Mentioned in GARTNER Market Guide API Security 2024

Gartner

OVERALL LEADER kuppingercole ANALYSTS

kuppingercole ANALYSTS

nasscom Emerge 50 Awards 2023

Winner of
Deep Tech Emerge 50 Awards
in the Cybersecurity category
for the year 2023

Most Innovative Product 2022 Winner

Most Innovative Product
of the Year-Winner 2022
Prophaze WAF 3.0

DSCI

Prophaze™
The New Phase of Security

# Deep Neural Networks & Self Supervised **AI/ML Modules**

## Development

- Static Code Analysis
- Software Composition Analysis
- Dynamic Application Testing
- Vulnerability & Penetration Test
- Happy Flow
- Traffic Profile

## Reduce False Positives

- Build Traffic DNA
- Create App Profile
- Hardened Zero Touch

## Production

- Automated Vulnerability Patch
- Run-time Protection
- Low Latency
- Zero Day Protection
- SIEM/SOAR Integration
- Legacy App Support

Tuned & Scaled for Enterprises

# Detect
## all Layer 7 calls

*No code change required*

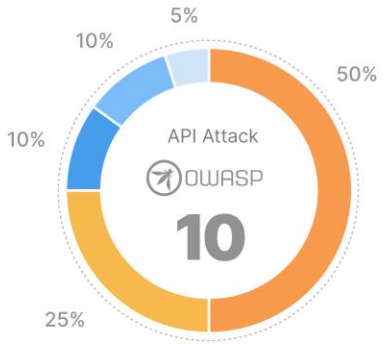
- Discovery
- Run Time
- Inventory
- Prevention
- Compliance
- Testing

# **Cohesive** Visibility & Control

Prophaze™ The New Phase of Security

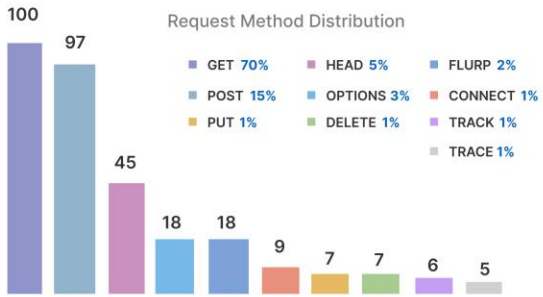
## Situational Awareness Focused Dashboard & Insights

Top API Attack Distribution




| | |
|---|---|
| A06:2021 - Vulnerable and Outdated Components | 36 |
| A09:2021 - Logging and Monitoring Failures | 36 |
| A06:2021 - Vulnerable and Outdated Components | 30 |
| A09:2021 - Logging and Monitoring Failures | 20 |
| A09:2021 - Logging and Monitoring Failures | 10 |

Top API Calls




### Comprehensive Protection

Monitor, authenticate, control access, and encrypt to prevent common API issues.

### Data Safeguarding

Ensure confidentiality, integrity, and availability with authorization, rate limiting, audit logging, and input validation.

### OWASP Defense

Shields against the latest OWASP API Security Top 10 threats, ensuring robust protection.

# Customised Rollout with Active Checks

## Guardrails

1. **Encryption (TLS 1.2+)**
   Protect data in transit
2. **Authentication (OAuth 2.0, JWT)**
   Validate user identities
3. **Authorization (RBAC)**
   Limit access to sensitive data
4. **Input Validation**
   Prevent SQL injections, Cross-site scripting (XSS), BOLA
5. **Rate Limiting**
   Throttle excessive requests
6. **API Key Management**
   Secure API Access
7. **Continuous Health Check**
   Regular Security Audits & Penetration Testing

## Imperatives

- Implement API Gateways
- Use API Security Standards (OWASP 10)
- Monitor API Performance and Security Metrics
- Continuously update API Security Policies

Prophaze™
The New Phase of Security

RE-INFORCED

API SECURITY

Tuned & Scaled for Enterprises

# Prophaze - Architecture Tuned for Enterprises

Prophaze™ The New Phase of Security

**Lowest** RoundTrip Latency

Traffic Orgin

Customer

Bad Actor

BOT

Browser

App

DNS

Firewall

DC - Prod

Layer 7 Traffic

Kubernetes Cluster/Pods

Virtual Patch

Application Servers

API GATEWAY

Output via APIs

RBAC Enabled GUI Controller for Prophaze

Real-time Dashboards

Executive Summary Reports

SIEM

SOAR

DC - Dev

DAST

SAST

Red Team

Build

Test

Deploy

Shift Left

**Handle TBs & beyond**

Top 25 Most Dangerous Software Weaknesses

OWASP TOP 10

# ....plus leveraging in house AI/ML Engine

## Agentless run-time protection for Applications & APIs

### Mid Market

- **Deploy in Minutes** - not months with zero config & downtime
- **Security Automation** - Automated protection for known/unknown vulnerabilities
- **Cost Effective** - remove additional expense on training & maintenance
- **Cloud Native** - Container supported deployments fits well with DevSecOps

### Enterprise

- **Application Aware** - Generates AI/ML profiles for applications independently
- **Self Learning** - Automated profiles based on incidents & AL/ML tech stack
- **Multi Cloud** - Supports Private/Public/Hybrid/On-Premise deployment
- **Customized Build** - Customized build based on domain specific use cases

## How it Works

### AI/ML Profiler

- Runs in background for a few days
- ML learns User & App behavior, API and container logic
- Profiles deep contents of payloads, static attributes of processes & files and previous threats

### Automated Policy

- Blacklisting
- Whitelisting
- Anomalies filtering
- Virtual Patching
- Threats updates

### DevOps Override Control

- Threat monitoring
- Block mode controls
- Custom rules
- API publishing
- Rate limiting
- Reports
- Integration options
- Events
- Alerts

Dynamic defense against never ending onslaught of attacks

Requires Zero configuration, tuning, or maintenance

Eliminates the cycle of breaches and patching