Prophaze
The New Phase of Security

Zero-Configuration Web Application and API Protection for Kubernetes

Zero-Configuration Web Application and API Protection (WAAP), DDoS protection and Bot Mitigation for Kubernetes leveraging AI Automation to keep businesses safe from targeted cyberattacks

- Defend web assets
- Ensure compliance
- Free from endless configuration and rules development
- Reduce security budgets

New Security Challenges

Many organizations are migrating to Cloud adopting new technologies but also exposing Web Services over the Internet to vulnerabilities that may compromise their entire systems. New solutions are needed to mitigate such new threats and security gaps.

Prophaze meets the challenge head-on to successfully defend against sophisticated cyberattacks, improve security posture, and lower total cost of ownership (TCO).

Problems	Solutions
Sophisticated AI Cyberattacks The rapid adaptation of sophisticated AI tools by bad actors have created an onslaught of unexpected stealthy attacks at a rapid rate. Clearly, the ability to craft payloads that pass undetected gives a tremendous advantage to attackers, making it difficult for security teams to scramble to identify and mitigate attacks from breaching corporate defenses, compromising customer data and damaging valuable brands.	**Blocking AI with AI** The most effective way to defend from AI attacks - is with an AI shield. Prophaze levels the playing field for security teams with an AI-powered application firewall to stop attacks at the gate and protect web-facing APIs and Microservices traffic across public and private clouds from cyberattacks in real-time. Prophaze security model is dynamic based on profiling context-based application behavior and static attributes of processes and files and does not require predefined rules. Instead, it infers rules through a learning process and blocks the execution of file-less attacks, new malware variants and zero-day attacks to only pass legitimate requests to the host server. The result is a holistic protection from threats, attack vectors, and application vulnerabilities, all in an easy to use and easy to deploy solution. (more in AI Adaptive Profiling)
Backward-looking Rule Setting A widespread mitigation technique is to deploy a Web Application Firewall (WAF), IDS, and/or IPS which attempt to detect malicious incoming payloads and drop them before they reach their target. However, these solutions are signature-based, rely on manual configuration of complex rules, or selection of pre-defined rules, to mitigate	**Automated Zero-Rules** Prophaze AI firewall eliminates the maintenance burden associated with legacy WAFs and static, rule-based solutions by automating the correlation and analysis required to identify real and active threats and implementing negative and positive security policy to mitigate vulnerabilities in deployed applications.

from known attacks, but are blind and exposed to unexpected attacks, causing an endless loop of backward-looking rule setting.	Prophaze adaptive architecture eliminates the need for in-house application security experts and achieves a higher degree of security without compromising your cloud deployment, breaking traffic or your budget.
Error-Prone Configuration Configuring and updating servers with rulesets often takes months to deploy, is cumbersome to manage, requires a significant effort to maintain and is prone to human errors and omissions causing vulnerabilities. Misconfigured settings are the most common problem exposing organizations to severe security and financial risks.	**Automatic Configuration** Prophaze AI automation eliminates the need for manual configurations which are prone to human error and shield organizations from the complexity of web application firewall, API protection and bot mitigation. Prophaze automatically creates and manages the entire security policy lifecycle: blacklisting, whitelisting, patching, response filtering, threat updates and more, while giving you override management to control specific activities and behavior of your applications.
Overloaded Operations CISOs are under significant stress of ever-increasing incidents, maintaining enterprise security and customer SLAs, HR issues, overworked security staff and difficult-to-fill expert positions at peak costs to maintain security operations.	**Managed Service** Prophaze does all the heavy lifting to secure enterprise web applications, eliminating the need for a large security staff or expensive resources while reducing your total operating security budget. Prophaze' ongoing managed service continuously adapts to the organization's web asset, ensuring it is always secure without the need for a dedicated team of experts.
Defense Gaps Corporate business departments often apply siloed security point solutions for detection and mitigation rather than prevention. This reactive approach to cyberattacks is costly and ineffective, complicates security operations and creates inherent gaps in security posture, leaving them unprotected from sophisticated attacks.	**Comprehensive Coverage** Prophaze provides comprehensive security coverage, proactively protecting the deployments from cyberattacks, mitigating vulnerabilities in the deployed applications and enabling seamless integration with other security solutions such as endpoint protection, CI/CD, SIEM, SOAR to share threat intelligence and to close any gaps in the enterprise-wide security coverage.

Prophaze
The New Phase of Security

Prophaze Solution

Real-Time Protection from Threats

Prophaze identifies, detects and blocks threats in real time, many of which go undetected by the traditional security technology stack:

- Misconfigured servers
- DDoS attacks
- MITM attacks
- Zero-day
- Malware attacks
- Brute force attacks
- Data Leak
- OWASP Top 10 Threats which include: Code and SQL injection, XSS, XXE, RCE, malicious payload headers and content, Cross-site forgery, Cross-site-scripting, File inclusion, Form manipulation, Cookie and session poisoning, Protocol exploits, DNS exploits, Path traversal, Credential stuffing, SSRF, CSRF, IP Reputation, Geo-IP Monitoring, Secure Session Management, .Net execution, MBR-based Ransomware, File less malware

Ensure Compliance

Many organizations find it difficult to maintain compliance due to lack of resources with unique expertise. Prophaze security compliance solution continuously monitors your web applications, APIs and configuration settings in real time to ensure compliance with many complex regulatory requirements and governance policies across your deployment such as HIPAA, GDPR, CCPA, SOC2, and PCI DSS.

AI Adaptive Profiling

Prophaze AI is a machine learning module based on proprietary Adaptive Profiling technology. It automatically correlates, analyzes and identifies malicious requests targeting your Web APIs and passes only legitimate requests. By deconstructing application logic and profiling payload contents, threats are categorized based on multiple attack detection algorithms and previous threat scores and dynamically translated into application-specific security policy: blacklisting, whitelisting, virtual patching, response filtering and blocking. Prophaze Adaptive Profiling provides protection from known threats including file-less attacks, new malware variants and zero-day attacks. Prophaze removes the need for lengthy investigations and ensures gaps in defenses are addressed.

Managed Security Updates

Prophaze Adaptive Profiling is a managed service updated daily with the latest global threats supported by thousands of international security researchers. Prophaze security policy and threat intelligence such as blacklisting of IPs discovered from malicious attacks on web Applications and Microservices can be easily shared with your security technology stack to improve your total security efficacy.

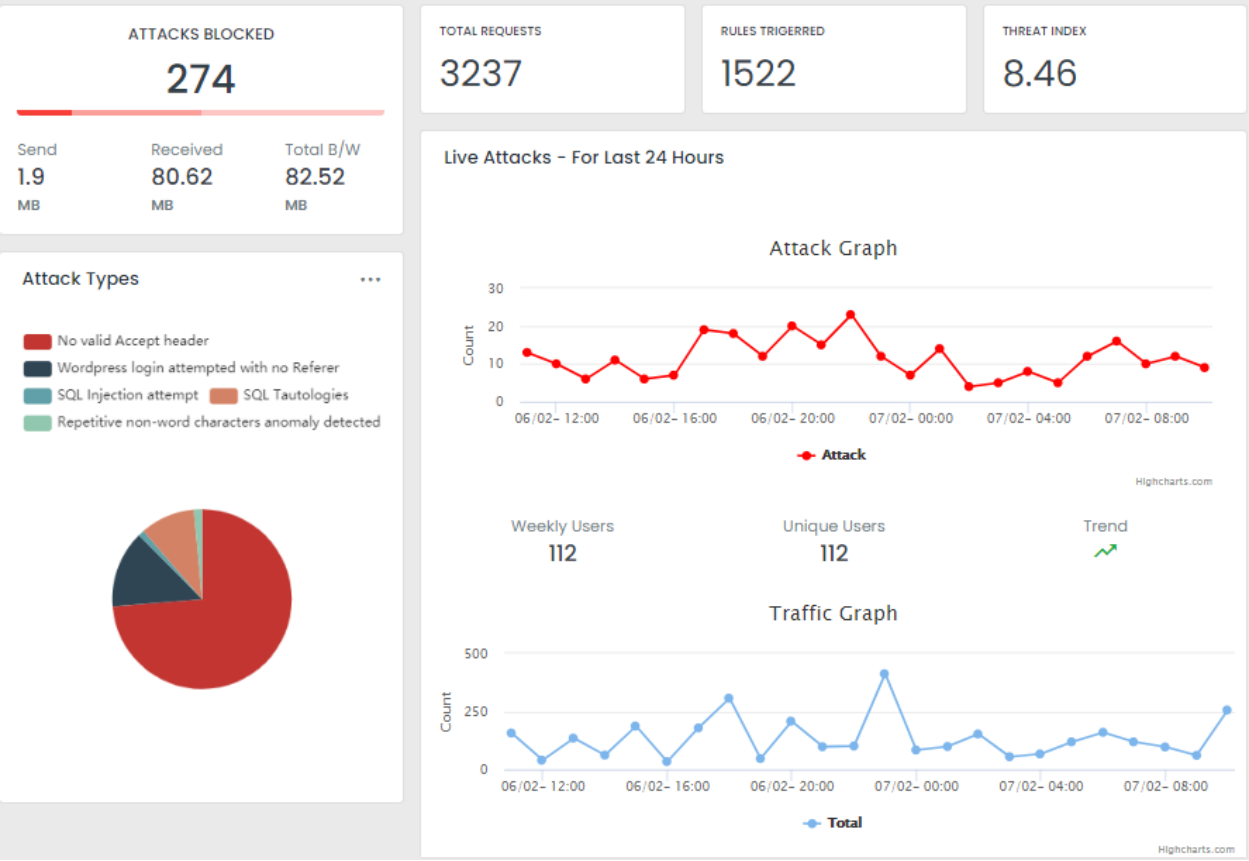
Any Cloud

Prophaze secures production deployments on public clouds, virtual private cloud environments such as AWS®, Google Cloud™ and Microsoft Azure® and hybrid clouds as well as on-premises IT infrastructure and datacenter with a single integrated solution.

Prophaze
The New Phase of Security

Intuitive, Real time Dashboard

Use a single interface to view, prioritize, investigate and manage in real time. Threat analysis is made simple with a few clicks to drill-down and investigate details, eliminating the need for complex workflows between products. The Prophaze dashboard provides compliance reporting and also live alerts via Slack and email interface.



Easy to Use

Prophaze solution is based on a fully automated, zero-configuration technology. Replacing the backward-looking signature decision-making mechanism, used by traditional WAFs and web security solutions, Prophaze applies AI weighted scoring system, based on context-driven inspection and behavioral modules. Prophaze continuously adapts to your workflow minimizing false positives, while freeing security teams from managing endless configuration and rules changes. Prophaze solution is easily deployed and scales with no need for changes to the organization's architecture.

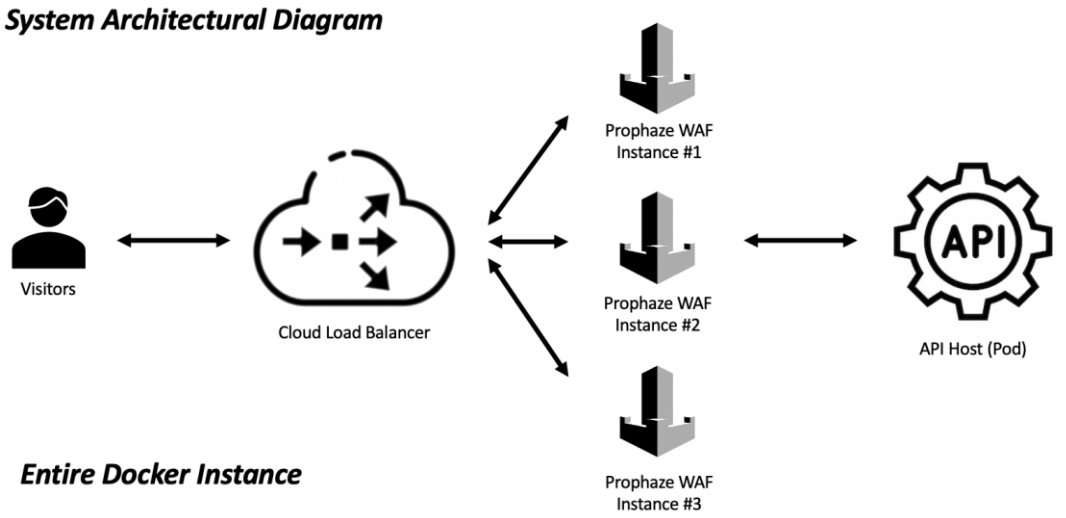
WAAP as a Service

To secure your API in real time, provide your APIs host address, change your API URL's A record to point to Prophaze address and submit basic information for account creation. It is that simple.

Native Kubernetes Firewall

Prophaze Helm Chart installation can replace your existing ingress controller with Prophaze custom ingress controller in zero down time. Prophaze is deployed in line with your Cloud load balancer as a Kubernetes microservice to inspect packets at ingress level towards API services.

Conversely, a Prophaze Kubernetes cluster can be deployed in the same zone as your AWS®, Google Cloud™ and Microsoft Azure® cloud instance provided that you want to keep your existing ingress controller. In this case Prophaze acts as a reverse proxy deployed at the DNS level which monitors API requests before reaching the Kubernetes cluster. This is different from conventional DNS Based WAF in the sense that technically the WAF is deployed on premise in your cloud data center. The WAF is deployed in your same AWS or GCP Region hence latency is negligible.



Private Cloud

Prophaze can be shipped as a Private Kubernetes Cluster which is installed behind your Load Balancer and can scale in accordance with instructions from the Load Balancer. The specification for the host needed for Prophaze WAF deployment is configured based on the total number of processed requests.

Extends Your Security Tech Stack

Prophaze works seamlessly with your existing security technology stack IDE, CI/CD, SCM, SIEM, SOAR, RASP, CDN, load balancers, reverse proxies, OpenAPI, Swagger files and is viewed as an incremental value add and best practice second line of defense to cover more threat vectors, increase efficacy and give the organizations a more comprehensive coverage of protection at the web facing endpoints.

Securing IoT APIs

Embedded Prophaze lightweight engine can be an integral part of a System on a Chip (SoC) on embedded Intel x86 or ARM CPUs with the full functionality of Prophaze and configured to the resource restrictions of the specific host system. For example, Prophaze can be loaded on Raspberry PI connected at the gateway of IoT interfaces to secure API endpoints such as CCTV and Advanced data fetching and parsing devices against OWASP Top 10 and other threats including zero-day attacks.

Prophaze Benefits

Large, Medium and Small Businesses

- Protects businesses of all sizes from Malicious Bots and Top 10 OWASP attacks.

- Managed service for businesses with limited or no security staff.
- Regulatory compliance for GDPR, HIPAA, CCPA, SOC2, PCI-DSS.
- Immediate time-to-value.

Enterprise Security Teams

- Protects deployments from misconfigured cloud exploits.
- Provides robust security in cloud environments and Kubernetes at scale reliably and cost effectively.
- Automates security policy. Completely eliminates the need for manual, error-prone configurations.
- Protects deployments from unknown vulnerabilities in SaaS, IaaS, PaaS solutions.
- Protects deployments from malicious bots bypassing legacy WAFs, CDNs.
- No traffic breaks. Agile DevOps can continuously update code without stopping for rule updates.
- Provides virtual patching before vulnerabilities can be fixed.
- Managed service protects businesses with limited or no security staff.
- Reduces security operation costs and budgets.
- Reduces hiring and training costs for DevOps.

SaaS

- Must-have solution for financial and healthcare customers.
- Protects customer SLAs which include security protection.
- Protects sensitive customer and personal data.
- Eliminates account data theft and prevents data leaks.
- Managed service protects services with limited or no security staff.
- Comply with costly regulations.
- Provides virtual patching during application lifecycle before fixes are available.
- Reduces security operation costs and budgets.
- Reduces hiring and training costs of DevOps.

Support and Professional Services

Technical Support

Our technical support combines years of enterprise security experience, proven application profiling analytics and security best practices expertise to help your Prophaze deployment through onboarding, implementation, questions and issues resolution. Chat support is available 24x7x365 via messaging, mail and Slack channels.

Professional Services

Security engineers are available 24/7 to assist with custom application security requests, troubleshooting and to resolve issues. Other services upon request include Secure Application Programming, Application Vulnerability Assessment, Technical Architecture Consulting and Application Penetration Testing.

Free Security Assessment

Prophaze offers a free security assessment of your web application deployed on a cloud platform to identify vulnerabilities, to avoid security breaches by malicious bots, DDoS, Top 10 OWASP and other threats. The assessment profiles your web server traffic, identifies behavior anomalies without interrupting the traffic or operations, and produces a vulnerability report with risk mitigation suggestions. Starting the assessment takes only a few minutes. To schedule your free security assessment, please contact us at checkup@prophaze.com.