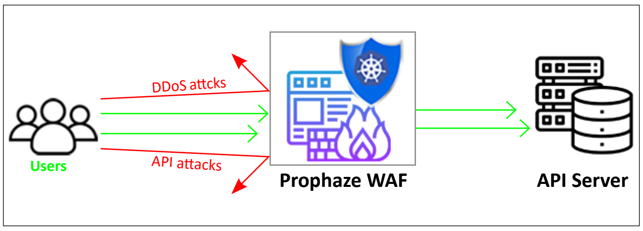
Prophaze
Web Security Platform

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 cyber-attacks, improve security posture, and lower total cost of ownership (TCO).



Sophisticated AI Cyber attacks

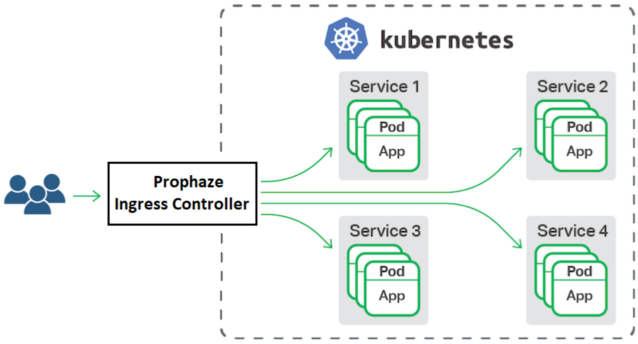
The rapid adaptation of sophisticated AI tools by bad actors have created an onslaught of unexpected stealthy attacks at a rapid rate. Clearly, the ability to craft payloads that pass undetected gives a tremendous advantage to attackers, making it difficult for security teams to scramble to identify and mitigate attacks from breaching corporate defences, compromising customer data and damaging valuable brands.

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

Prophaze WAF defends applications from known vulnerabilities and from zero-day threats. It provides high performance, supports physical or virtual appliances and containers deploy on-site or in the public cloud to serve any size of the organization (from small businesses to service providers, carriers, and large enterprises).

Kubernetes Ingress WAF by Prophaze is a Kubernetes Native Web Application Firewall (WAF) which intelligently tracks down malicious request into your Web APIs. It uses multiple attack detection algorithms to monitor all the incoming requests and will pass only legitimate requests to your micro-sing machine learning to model each application, Prophaze defends applications from service.



FEATURES

Web Application Protection

Multi-layer protection against the OWASP Top 10 application attacks uses machine learning to defend against known and unknown attacks. Thus securing customer data Providing 100% security compliance.

API Protection

Public, private, or partner-facing APIs have a key role in accelerating digital transformation. However, many organizations, including large enterprises, have relatively immature API security programs, thus creating a completely new attack surface.

Your DevOps team can validate and deploy secure custom APIs based on OpenAPI specifications directly from the dashboard. Prophaze creates a positive security model to validate only the traffic that has to access your APIs. Thus protecting all your API endpoints. Prophaze API security is vendor-agnostic supporting the leading API gateways.

Protect your APIs from malicious actors by automatically enforcing positive and negative security policies. Seamlessly integrate API security into your CI/CD pipeline.

Layer 7 DDoS Mitigation

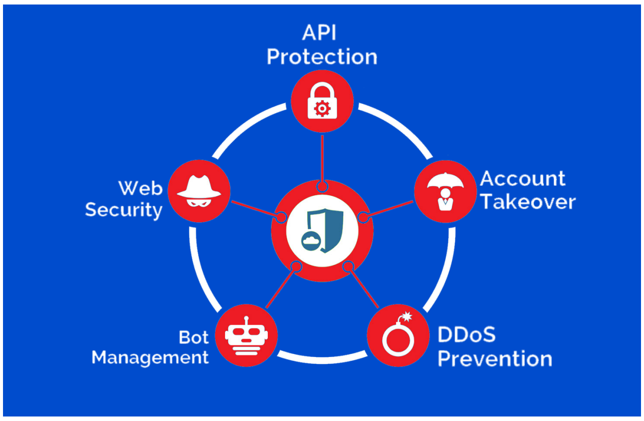
Prophaze can defend well against Layer 7 DDoS attack where legacy solution's capability stops at rate limiting. Prophaze behavioural learning capability can make sure that infrastructure is rate limited to Bad actors and makes no service interruption to legitimate users.

Bot Mitigation

Prophaze BotCry is an advanced machine learning based Bot Mitigation solution. It can fight against other ML based malicious bots which do targeted and automated attacks against web APIs and applications.

SD-WAF

Prophaze is having the first software-defined web application firewall (SD-WAF) in the industry. The entire web security platform is tailored into infrastructure as a service and deployed as a script on the Kubernetes platform. There by it makes the deployment in just a matter of minutes, everything can be deployed and up can be running. This makes Prophaze WAF very scalable and robust platform.



Dedicated SSL Certificates

Prophaze automatically provisions SSL certificates that are shared by multiple customer domains. Prophaze validates the device's certificate to verify whether it has authorized access to the endpoint, while a user tries to establish a connection with its origin server. TLS Client Auth (Mutual Auth) creates a secure connection between a client such as a device / mobile app and its origin.

KEY CAPABILITIES:

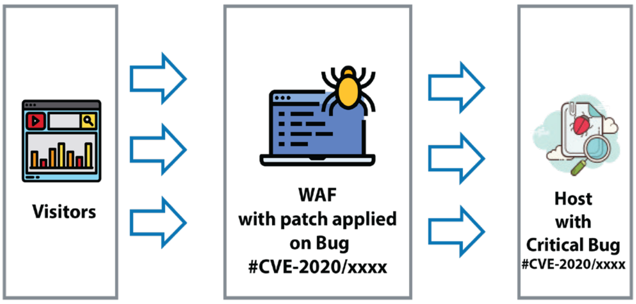
- Secures your website against hacking.
- Protecting your Brand against Breaches.
- Machine learning that detects and blocks threats while minimizing false positives.
- Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users.
- Dynamic profiling learns protected applications and user behaviour, thus automatically applying a positive security model.
- Flexible deployment to support hybrid environments (on-premises and cloud).
- Updates web defences with research-driven intelligence on current threats .
- Visual analytics tools for advanced threat insights.
- Fully PCI compliant simplified event investigation with Attack Analytics.
- Correlates security violations to detect sophisticated, multi-stage attacks.
- Automated Virtual Patching .
- High performance, transparent, drop-in deployment .
- Defending your web apps against sophisticated denial of service attacks.

Deployment Options

The Prophaze WAF can be deployed in any Public cloud such as AWS, GCP, Azure, Digital Ocean and on Private Cloud instance like Microk8s.

Virtual Patching

Prophaze automatically deploys virtual patching to web applications, APIs and microservices to block malicious traffic from exploiting vulnerabilities before the application source code can be modified. Considering the critical situation when organizations can't immediately edit the source code, makes the value of virtual patching significant.



Compliances

Commerce, FinTech, Health Tech, and organizations that process PII and PHI data find it difficult to maintain compliance due to lack of resources with unique expertise.

Prophaze compliance solution protects your web applications, APIs, and configuration settings in real-time to ensure that your APIs exposing PII data comply with GDPR, HIPAA, CCPA, PCI-DSS and SOC2 and other complex regulatory requirements and governance policies across your deployment.

INTEGRATIONS

Prophaze extends your security tech stack by routing notifications directly to communication products like Slack and Microsoft Teams. Other integration platform include security and event management (SIEM) products like Splunk, to security monitoring solutions like Datadog. It also sends alerts via webhooks to existing workflows, and export events in various formats like syslog messages, Common Event Format (CEF) and JSON format.

SIEM – Splunk
Monitoring – Datadog
Communications – Slack, Teams