Prophaze **EagleEYE**

New phase of security

EagleEye is a web application firewall (WAF) that secures your hosted web applications from attacks and Vulnerabilities. Using Artificial Intelligence based attack detection method along with multidimensional protection including daily updated threat signatures, Rate Based filtering and custom rules, EagleEye offers you a threat free environment.

Performance and speed

EagleEye load balancing enables organisation to be more cost effective along with the capabilities of an enterprise grade SLA platform.

Web Application Protection

With the help of EagleEye's industry leading WAF technology, any type of web threats including OWASP Top 10 threats can be handled easily.

Account Management

Experts at Prophaze will work with you on complex setup, integration and customisation requirements to ensure your security and to see that your operational goals are met.

AI (Artificial Intelligence) and BigData Powered tools

AI-powered platform learns from your traffic to deconstruct application logic and create application specific rules.
Lowers false-positives by customizing security rules to the application logic New threat vectors via Easily imported ruleset recommendations

Highlights

* AI-based behavioral scanning for threat detection
* Layer 7 server load balancing Caching
* Attack analytics for advanced threat insights
* Third-party integration and virtual patching
* Live treat Updates through premium sources

Customised setup and branding

We provide customisation options to enterprises so that they can easily brand customer facing pages so as to reflect their own website's look and feel.

Premium 24 * 7 Support

The dedicated team at Prophaze will provide you support round the clock whenever it is needed.

HIGHLIGHTS

Web Application Security with EagleEye

Prophaze has a complete understanding about the world of enterprise web Application which helps to work closely with enterprise IT teams and to meet their specific integration and customization requirements. The end-to-end application delivery service maximizes the security and performance of websites and web applications as it is backed by an enterprise-grade up time SLA and premium support.Thus Prophaze helps enterprises in cost reduction and simplification of their IT processes by consolidating multiple appliances and services into a single cloud based solution.

Artificial Intelligence based behavioral scanning for threat detection

AI-powered platform learns from your traffic to deconstruct application logic and create application specific rules. Lowers false-positives by customizing security rules to the application logic New threat vectors via Easily imported ruleset recommendations

Integration with T hird-Party Scanners

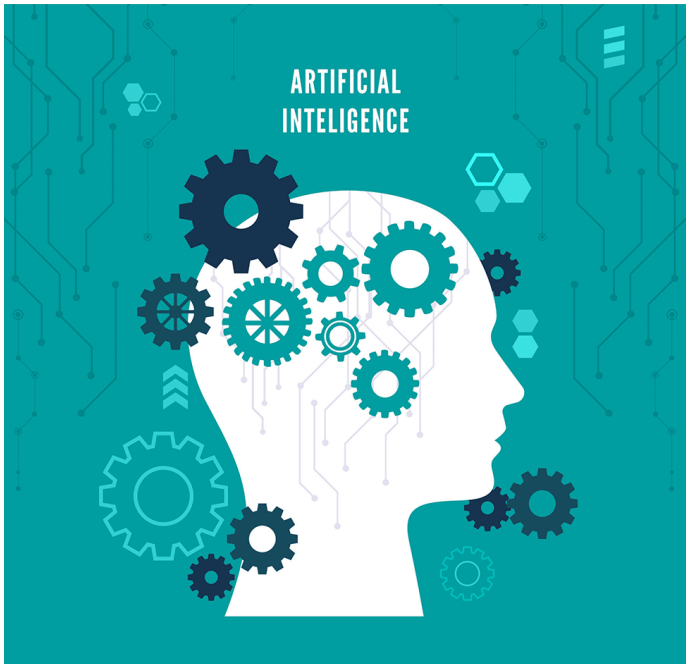
EagleEye's adaptive profiling and integration with third party security scanners like Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar, and WhiteHat is used to create dynamic rules as soon as a vulnerability is detected by the scanners

Solving the Challenge of False Threat Detections

EagleEyes AI based Machine Learning Algorithms can reduce both false positives and negatives to a great extend . Combined Threat Score , weightage fingerprinting EagleEye can provide nearly 100% anomaly detection

API Security

Since recent years , API based application to application communication is increased as the necessity of interfacing and integration with different systems , formats and protocols are increased



VM and Public Cloud Options

Deploy Prophaze WAF on-premises with the same set of security policies and management capabilities It also integrates easily with popular cloud services such as Amazon Microsoft Google or as a cloud service itself as reverse proxy

Advanced Graphical Analysis and Reporting

EagleEye helps to detect threats, outages and eliminate downtime by using the Real time analysis, health and performance checks of server activity. The system can be fine tuned to receive email alerts for any incident scenarios. EagleEye proactively takes care of potential issues on the fly before they affect your website users. It is done by using the Real time dashboards which intelligently analyze the attack vectors and verify that your Traffic is safe

FEATURES

Deployment options
- Dedicated Server
- Reverse Proxy
- Amazon AWS
- Microsoft Azure
- Google Cloud

Web Security
- HTTP Compression
- HTTPS/SSL Offloading
- Content Routing
- Layer 7 server load balancing
- Caching

Web Application Security
- OWASP Top 10 Signature
- OWASP Automated Threats Signature
- Application Learning (Adaptive Profiling)
- DoS prevention
- Server Cloaking
- URL Encryption
- Geo-IP Monitoring
- IP Reputation Checking
- Operating system intrusion signatures
- Web services signatures
- WebSocket protection
- Man in the Browser (MiTB) protection
- Cross Site Request Forgery
- Threat scoring and weighting
- Syntax-based SQLi detection
- Custom error message
- Data leak prevention

Cybersecurity Essentials
- Whitelisting
- Blacklisting
- Session Hijacking
- Protocol validation
- HTTP/HTTPS encryption
- HTTP Header Security

Attack detection
- AI (Artificial Intelligence) and BigData Powered
- Dynamic application profiling
- Proxy level
- Application level
- Page level
- Form level

Application Attack Protection
- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration

Management and Reporting
- Web user interface
- Prophaze graphical analysis and reporting tools
- Active/Active HA Clustering
- Centralized logging and reporting
- Predefined security policies for Drupal and Wordpress
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics

Thank You

Prophaze Technologies Pvt Ltd.
security@prophaze.com
+91 7994008420