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 Multi dimensional 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 Organization 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 customization 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.

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 and error code
- Data leak prevention

Cybersecurity Essentials

- Protocol validation
- Session Hijacking
- HTTP Header Security
- HTTP/HTTPS encryption

Attack detection

AI (Artificial Intelligence) and BigData Powered tools
Dynamic application profiling learns all levels from

- 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
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- Predefined security policies for Drupal and Wordpress applications

Thank You

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