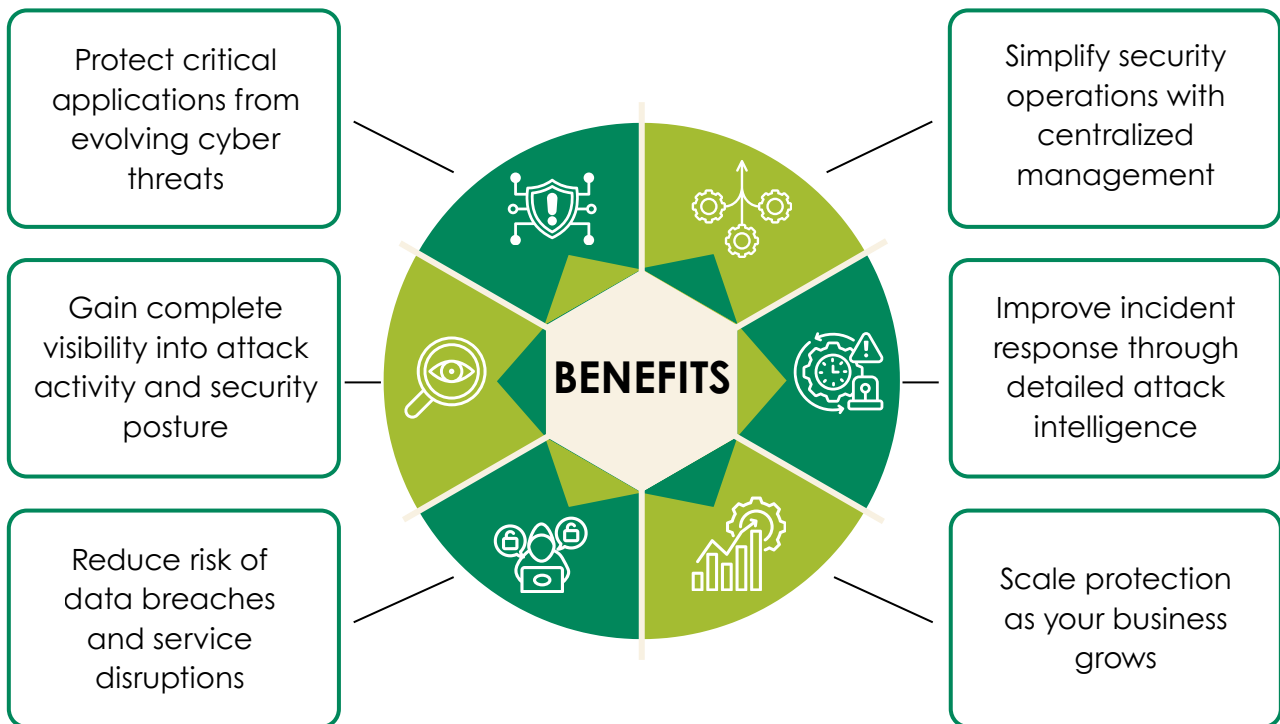




# Huracan Wall

Advanced Web Application Protection for Modern Businesses

HuracanWall is a powerful, enterprise-grade Web Application Firewall (WAF) designed to safeguard web applications, APIs and online services from sophisticated cyber threats. Combining intelligent threat detection, real-time protection, and centralized management, HuracanWall enables organizations to secure critical digital assets with confidence.



## WHY HURACAN WALL?



HuracanWall delivers enterprise-grade web application security with powerful protection, actionable visibility, and operational simplicity. It empowers organizations to defend their applications, monitor threats in real time and maintain business continuity in an increasingly hostile cyber landscape.

# Huracan Wall

## Key Features

|                                                  |                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Real-Time Threat Detection and Prevention</b> | <ul style="list-style-type: none"><li>Identifies and blocks web application attacks before they reach your servers.</li><li>Protects against <b>OWASP Top 10 threats</b>, including SQL Injection, Cross-Site Scripting (XSS), Remote Code Execution, Path Traversal and more.</li><li>Detects both known attack signatures and suspicious behavioural patterns.</li></ul> |
| <b>Comprehensive Attack Visibility</b>           | <ul style="list-style-type: none"><li>Detailed attack intelligence with complete event breakdowns.</li><li>View attack type, source IP address, targeted application, request details and malicious payload information.</li><li>Enables rapid investigation and incident response.</li></ul>                                                                              |
| <b>Centralized Security Dashboard</b>            | <ul style="list-style-type: none"><li>Intuitive web-based management interface.</li><li>Single-pane visibility.</li><li>Real-time monitoring of security events, traffic trends and policy enforcement.</li></ul>                                                                                                                                                          |
| <b>Simplified WAF Configuration Management</b>   | <ul style="list-style-type: none"><li>Easily create, modify, and enable WAF configuration &amp; reverse proxy settings through a user-friendly interface.</li><li>Manage protection rules without requiring deep security expertise.</li><li>Flexible rule tuning for performance while maintaining strong protection.</li></ul>                                           |
| <b>Advanced Logging</b>                          | <ul style="list-style-type: none"><li>Detailed security logs for auditing, and threat analysis.</li><li>Search and filter events by attack type, source, application, severity and time range.</li><li>Supports long-term retention of security events for investigations.</li></ul>                                                                                       |
| <b>Intelligent Attack Classification</b>         | <ul style="list-style-type: none"><li>Automatically categorizes threats based on attack vectors and severity levels.</li><li>Prioritizes critical threats to help security teams focus on the most significant risks.</li><li>Clear and actionable attack descriptions for faster automated decision-making.</li></ul>                                                     |
| <b>API and Web Service Protection</b>            | <ul style="list-style-type: none"><li>Secures modern APIs and web services against abuse and exploitation.</li><li>Monitors inbound requests for malicious payloads and anomalous behaviour.</li><li>Helps maintain service availability and application integrity.</li></ul>                                                                                              |
| <b>High-Performance Traffic Inspection</b>       | <ul style="list-style-type: none"><li>Inspects application traffic with minimal impact on performance.</li><li>Designed to support high-traffic environments and business-critical applications.</li><li>Scales seamlessly as organizational requirements grow.</li></ul>                                                                                                  |
| <b>Selectable Attack Rules</b>                   | <ul style="list-style-type: none"><li>Select desired rules as per orgs web asset protection policies and enforce actions.</li><li>Adapt quickly to emerging threats and unique application environments.</li></ul>                                                                                                                                                         |
| <b>Flexible Deployment Options</b>               | <ul style="list-style-type: none"><li>Suitable for on-premises and private cloud.</li><li>Integrates seamlessly (inline) into existing network and security architectures.</li></ul>                                                                                                                                                                                       |



## Stay Connected

+92 51 8852888

info@quantumronics.com

+92 321 9112230

107, First Floor, Evacuee Trust Complex,  
Agha Khan Road, F-5/1, Islamabad