LIMELIGHT CLOUD WAF SERVICE

The combination of the Cloud Web Application Firewall (WAF) solution and the Limelight Edge Services Platform is the perfect combination to combat the sophistication of today’s attacks, providing a protective shield around your security perimeter. Leveraging our cloud-based network resources delivers cost effective protection for your web applications without a performance penalty.

CHALLENGES PROTECTING YOUR WEB APPLICATIONS

Web application development is becoming increasingly complex and more rapid. With application availability more important to the user experience than ever, web applications are becoming increasingly vulnerable, exposing enterprises to the risk of data breach and financial loss. Web application security is already a critical area for organizations of all sizes. Retail and financial sectors suffer the most from web app attacks, and over the past year there has been a significant increase in attack incidents, increasingly from malicious bots, with web sites containing consumer data being a prime target of attacks. The cost and complexity of preventing and responding to attacks is on the rise, so only a comprehensive suite of global cloud-based security services, rather than on-premise equipment, allows you to keep abreast of the latest threats and preventive mitigation measures without impacting performance of your web application infrastructure.

HOW THE LIMELIGHT CLOUD WAF SERVICE SOLVES THE CHALLENGES

The Limelight Cloud WAF Service provides robust application security by uniquely using a positive security model in addition to a negative model. Automatic machine-learning technologies analyze traffic to learn what constitutes normal legitimate behavior, and automatically blocks activity that is not permitted or is outside normal behavior. This provides comprehensive protection against Open Web Application Security Project (OWASP) Top 10 threats and unknown vulnerabilities such as zero-day attacks, with a minimum of false positives. Any false positives are automatically detected and corrected. Dynamic protection policies are automatically generated by application mapping of protected apps, to detect changes whenever new features are added or modified, and identify potential vulnerabilities. Continuous detection of changes in the applications, and acceptable user behavior, keep protection current. The Cloud WAF Service also includes advanced bot mitigation to identify malicious bots based on unique device characteristics. These unique fully-managed Cloud WAF Security services with continuously adaptive security policies, provide the strongest web application security.

LIMELIGHT CLOUD WAF SERVICE FEATURES

The Cloud WAF Service provides powerful defenses against HTTP application layer threats through a variety of compelling capabilities:

Robust Global Cloud Security Network—5 Tbps of global mitigation capacity with dedicated scrubbing centers provide low latency proximity to WAF nodes for a performance optimized solution.

Complete Protection Against OWASP Top 10 Threats—A positive security model uses advanced behavioral analysis to detect malicious threats, including unknown vulnerabilities such as zero-day attacks.

Automatic Correction of False Positives—Powerful machine-learning algorithms learn to identify legitimate application behavior.

Continuously Adaptive Security Policies—Continuously maps applications, detects changes in them, and dynamically deploy the optimal security policy.
Advanced Bot Mitigation—Unique device fingerprinting identifies malicious bots based on multiple device characteristics.

Data Leakage Prevention—Masks sensitive user data such as credit card numbers, ID numbers, SSNs, and other Personally Identifiable Information.

Built-in DDoS Protection—Up to 1GB of traffic protection.

Behavioral L7 DDoS Protection—Uses behavior-based mechanisms that don’t rely on rate limits, resulting in very few false positives.

Dashboard and Reporting—Rich centralized dashboard to display threats and manage configuration, and reporting for both WAF and DDoS protection.

Fully-Managed Security Service—By the Expert Response Team (ERT) of experienced security experts.

BUSINESS BENEFITS
Limelight Cloud WAF protection gives you the following benefits:

Faster Time to Security—Advanced automation technologies instantly detect attacks and respond on-the-fly to reduce exposure.

Complete Protection—Positive security model combined with continually adaptive and dynamic security policies provides the industry’s best web application protection.

Reduced Overhead—Automated WAF defenses with fully managed services remove a burden off IT personal and provide better security.

Eliminates Sacrificing Performance for Security—WAF nodes only accept traffic from the CDN, so only see the dynamic traffic that potentially contains attacks.

ABOUT LIMELIGHT NETWORKS
Limelight Networks, Inc. (NASDAQ: LLNW) is a global leader in delivering the highest quality online video experiences and edge-enabled workflows. Limelight’s edge services platform makes knowledge, information, and entertainment instantly accessible anywhere in the world and accelerates the next generation of real-time, interactive and immersive content. For more information, visit www.limelight.com, follow us on Twitter, Facebook, and LinkedIn.