LIMELIGHT CLOUD SECURITY SERVICES

Limelight Cloud Security Services use the Orchestrate Platform’s global reach to secure content and mitigate attacks on your website and web servers. They include encrypted content delivery and multiple access control methods that enable you to protect your digital assets.

CHALLENGES SECURING AND PROTECTING YOUR CONTENT

Ensuring a great quality of experience for users entails securing and protecting content from a variety of potential threats. With the cost and complexity of preventing and responding to security breaches on the rise, only a comprehensive suite of global cloud-based security services allows you to keep abreast of the latest threats and preventive mitigation measures without adding latency to the delivery experience.

HOW LIMELIGHT CLOUD SECURITY SERVICES SOLVE THESE CHALLENGES

Limelight Cloud Security Services provide powerful features to protect against attacks on websites and control access to content. Security of content in transit against theft is provided by the largest SSL footprint, and website access authorization is controlled by geo-fencing, URL tokenization, and IP address white and black listing so you can enforce licensing restrictions and prevent theft of content.

Defensive Protection—Passive attack mitigation via massive CDN.
SSL / HTTPS Delivery—Deliver digital assets securely via the largest SSL global footprint.
Customer Certificates—Host customer’s SSL certificates.
Geo Fencing—Control access based on geolocation.
DDoS Attack Interceptor—Detect and mitigate attacks against websites.
MediaVault—Tokenization-based video stream access control.

Cross Origin Resource Management (CORS)—Allow multiple content sources while restricting sharing to designated origins.
IP Whitelisting and Blacklisting—Control access based on IP addresses.
Small Web Format (SWF) Verification—Authorizing which files can connect for playback.
Web Application Firewall (WAF)—Cloud-based globally distributed infrastructure integrated with the CDN, identifies and blocks attacks.

LIMELIGHT SECURITY ALERT

Security Alert adds the following features to our standard Cloud Security Services:

- Globally Distributed Anycast Addresses—Ensure large attacks are distributed to multiple Limelight POP locations rather than a single POP for improved mitigation.
- DDoS Attack Notification and Alerts—Attacks are detected and communicated through an email-alert, providing awareness so that appropriate measures can be taken to defend their valuable assets.

LIMELIGHT WAF COMPLETE

WAF Complete includes Security Alert and capabilities and adds these additional security features:

- Per IP Address Rate Limiting—Control the maximum number of requests per second from a single IP address.
- CAPTCHA Support—Protect websites against bots and scripts by requiring human logic.
- Access Control—Block access based on IP address, or geographic location.
- Intuitive User Portal—Allows customers to easily turn specific WAF features on or off, and easily view important data related to the WAF.
- Basic OWASP 10 Rules—Origin is shielded by the CDN and traffic filtering by the WAF which covers the OWASP Top 10.
- Fully managed White Glove Service—Limelight security experts assist in the setup and configuration of the WAF and its associated rules.
- Active Mitigation of Layer 7 DDoS Attacks—Multiple defenses deployed to protect web applications including good bot/bad bot detection, IP rate limiting, IP access control, and CAPTCHA challenges.
• **Bad Bot Detection and Mitigation**—Incoming requests for content are challenged and fingerprinted to determine if generated by bot/script or human user.

• **Access Control**—Access rules based on IP addresses, location of the end user, browser type, and URL being accessed.

• **Custom WAF Rules**—Custom rules on a per web application basis, created by description of vulnerabilities and how detected.

• **Access to WAF Portal and Reports/Data**—Dashboards in control displays WAF rules state, requests alerted, and request handling.

• **24X7 Security Operations Center Monitoring**—Daily threat intelligence monitoring, vulnerability and threat analysis, full threat simulation and regression testing.

---

**LIMELIGHT DDoS ATTACK INTERCEPTOR**

DDoS Attack Interceptor provides a powerful solution to the threat of cyber-attacks through a variety of compelling capabilities.

• **Passive Mitigation**—Limelight’s distributed network of data centers provides enormous capacity to absorb attacks that are not complex enough to be moved to scrubbing.

• **Detection of Network Layer Attacks**—Using behavior-based analysis, DDoS Attack Interceptor intelligently detects attacks even when a signature does not exist, offering protection from a broad spectrum of attack types in addition to network based attacks (Layer 3, 4).

• **In-network Detection**—DDoS Attack Interceptor actively monitors for DDoS attacks so you don’t have to. Proactive detection shortens response times and allows mitigation to begin quickly.

• **Automatic Mitigation**—Attack traffic is mitigated by the Security Operations team by diverting it to globally distributed scrubbing centers, giving you the protection you need, when you need it, without having to install costly security appliances locally.

• **Bill Shock Avoidance**—Mitigation of attack traffic means you only pay for filtered traffic, avoiding costly overcharges due to a DDoS attack.

• **Access to the DDoS AI Portal**—View available realtime data regarding attack detections and mitigations, while historical attack data and threat intelligence reports allow you to identify trends and plan for the future.

• **Flexible Deployment**—DDoS protection services are easy to activate and manage – which means no new hardware or software and no changes to your web applications.

• **24X7 Monitoring**—Covered shortname/anycast address for potential DDoS attacks.

---

**BUSINESS BENEFITS**

Choose the best approach with cloud-based security services:

**Web Applications and Origins are Protected**—Massive global network absorbs traffic flooding.

**High Performance Mitigation**—On Network scrubbing maintains performance even under attack.

**Compliance with Copyright Protection**—URL tokenization limits access to licensed content, keeping unauthorized users off corporate websites.

**Maintain Brand Perception and Revenue**—Block network attacks with globally distributed DDoS AI and WAF protection mechanisms, performance is not sacrificed for security, and your websites are available for business.

---

**ABOUT LIMELIGHT NETWORKS**

Limelight Networks Inc., (NASDAQ: LLNW), a leading provider of digital content delivery, video, cloud security, and edge computing services, empowers customers to provide exceptional digital experiences. Limelight’s edge services platform includes a unique combination of global private infrastructure, intelligent software, and expert support services that enable current and future workflows. For more information, visit www.limelight.com, follow us on Twitter, Facebook, and LinkedIn.