

Limelight Web Application Firewall Enhancement

ライムライトのコンテンツデリバリーネットワーク(CDN)とWebアプリケーションファイアウォール(WAF)の統合は、現代の先進的なサイバー攻撃に対抗するための理想的なソリューションを提供します。ライムライトのクラウドベースのネットワークリソースを活用することで、パフォーマンスを犠牲にすることなく、Webアプリケーションをプロアクティブ、効率的かつ低コストで保護することができます。

主な機能

WAFは、HTTPアプリケーションレイヤーの脅威に対して強力な防御が可能な特別なファイアウォールです。これを独自のクラウドCDNソリューションと統合したLimelight WAFには、以下の様な機能があります:

- **専用のグローバルネットワーク** – 世界中に分散して配置されたライムライトのネットワークデータセンターは、WAFノードに対して低レイテンシのプロキシとして働き、パフォーマンスを最適化します。
- **オリジンの保護** – 全てのトラフィックは、オリジンのサーバーに到達する前にWAFを経由します。
- **ボットネットへの対抗** – ブラウザの機能をテストするアルゴリズムを使って、本物のブラウザかボットネットの行動かを見極めます。
- **Webアプリケーションセキュリティポリシー** – トラフィックは、Open Web Application Security (OWASP)から配信されている重要度の高いセキュリティリスクのルールに基づいてフィルタされます。
- **アプリケーション特有のルール** – 個々のWebアプリケーションの脆弱性をカバーするための特別なルールを適用できます。さらに、Webアプリケーション毎にカスタムに作成したルールも適用可能です。
- **新しい脅威からの影響の緩和** – 脅威インテリジェンスからの情報を自動的にアップデートし、新しい脅威を解析することで、全てのWAFノードに新しいセキュリティルールを配信します。
- **ダッシュボードとレポート** – 特定のWebアプリケーションについて、防御とアラートについてのハイレベルな状況を表示します。また、ウィジェットを使って特定のIPやルールセットについてドリルダウンし、潜在的な脆弱性について確認できます。
- **詳細な攻撃ログ** – ハイレベルのアラートや指標から、詳細な情報へドリルダウンできます。
- **アクセス制御** – IPのホワイトリスト化/ブラックリスト化、及び地域によるアクセスルールを設定できます。
- **WAFコントロールセンター** – ハイレベルな視点から、脆弱性データを可視化します。
- **リアルタイムSIEMサポート** – Security Information and Event Management (SIEM)を使っている組織では、WAFが収集したイベント情報をSIEMからも利用できます。

Webアプリケーションを守る上での課題

Webアプリケーションをどう守るかということは、既にあらゆる規模の組織で重大な問題となっています。例えば、小売り及び金融業界はWebアプリケーションへの攻撃の影響を最も受けている業界です。これらの業界への攻撃インシデントは、ここ数年間飛躍的に増加しており、その60%はWebサイトに含まれるコンシューマデータを狙っています。

攻撃を予防し対応するためのコストと複雑さが増え続けていますが、セキュリティ予算はサイバー被害へのリスクに見合うほど増加していないのが実情です。こういった状況に、オンプレミスの機器だけでは対抗できません。グローバルなクラウドベースの包括的なセキュリティサービスのみが、最新の脅威に追従し配信体験に影響を与えずに予防的緩和措置をとることができます。

Limelight Web Application Firewall Enhancement

Limelight WAFで課題克服

Limelight WAFのノードは、オリジンサーバーとライムライトCDNの間に位置しています。CDNはコンテンツキャッシュ、Webの高速化及び静的コンテンツの配信に関して重要な役割を担っていますが、Webアプリケーションを狙う攻撃は動的なため、CDNは動的なトラフィックのみをWAFノードに転送します。WAFがCDNからのトラフィックのみを受け取ることで、全体のパフォーマンスに与えるインパクトを最小化し、解析すべく減少させることができます。

WAFは、Open Web Application Security Project (OWASP)が提供しているアプリケーションセキュリティリスクのためのトップ10ルールをトラフィックに適用し、攻撃を検知します。さらに、セキュリティオペレーションセンターは新しい脅威についての闇ブログやBBSを監視しており、新たな脆弱性が特定されると、新しいセキュリティルールが作成され、全てのWAFノードに配信されます。

例え「ゼロデイ」攻撃であっても、アプリケーションベンダーが対応する前に攻撃を遮断できます。スケーラブルなクラウドベースのアーキテクチャが、WAFサービスの低コストな保護を支えています。

ビジネスメリット

Limelight WAFによる保護には、以下のようなメリットがあります:

- コンテンツを盗難から保護 — 世界中に分散された拡張性の高いインフラとOWASPのフィルタルールにより、Webアプリケーションを攻撃から守ります。
- 保護のためのトータルコストを削減 — クラウドベースのアーキテクチャによって検知機能を世界中に分散し、効率を高めます。
- パフォーマンスを犠牲にしないセキュリティ — WAFノードはCDNからのトラフィックのみを受信し、攻撃を含んでいる可能性のある動的トラフィックのみを監視します。
- 監視とレポート — 包括的なアクティビティダッシュボードにより、潜在的な脅威と脆弱性を可視化し、それには日々の闇ブログの監視結果も反映されます。

Limelight Networksについて

Limelight Networks (NASDAQ: LLNW) は、デジタルコンテンツ配信のグローバルリーダーです。デジタルコンテンツを管理し、世界中の多種多様なデバイスに送り届けることで、お客様がオンラインの視聴者とよりよい関係を築くためのお手伝いをしています。詳しくは jp.limelight.com をご覧下さい。

Limelight Networks および当社のサービスの詳細についてはこちらまでお問い合わせください。

ライムライト・ネットワークス・ジャパン株式会社

〒107-0061 東京都港区北青山2-7-28 NAビルディング2F

TEL: 03-5771-4230

info-jp@llnw.com ■ jp.limelight.com