imperva

機能のご紹介

クラウドウェブアプリケーションファイアウォール

クラウドにおけるアプリケーションセキュリティ

フォーチュン500の大手企業は、自社のウェブアプリケーションを頼りに収益を上げ、望ましいブランドイメージを構築して、顧客関係を育んでいるため、現代のウェブアプリケーションはミッションクリティカルな存在となっています。しかし、こうした企業は、世界中のあらゆる地域から発生するセキュリティ脅威に直面しています。サイバー犯罪者は、企業のデジタルプレゼンスを利用してそのIT環境に足がかりを作り、貴重な企業データへのアクセスを試みています。さらに、ウェブアプリケーションソフトウェアのアジャイル開発プラクティスへの移行によって、ソフトウェアが入念にテストされず、サイバー犯罪者に悪用されかねない重大な脆弱性を抱えたままリリースされる可能性が高まります。企業は、包括的なセキュリティ保護のみならず、世界中のユーザーに合わせて柔軟な拡張性を提供できる、ウェブセキュリティソリューションを求めています。

Imperva Cloud WAF

Imperva Cloud WAFは、業界トップのウェブアプリケーションセキュリティファイアウォールを提供することで、最も複雑なセキュリティ脅威に対してもエンタープライズクラスの保護機能を実現します。ウェブサイトやアプリケーションをパブリッククラウドまたはオンプレミスでホスティングしている場合でも、Cloud WAFはアプリケーション層を狙ったあらゆる種類のハッキングから重要なアセットが確実に保護されるようにします。

Cloud WAFは、統合型多層防御のアプリケーションセキュリティおよびデリバリーサービススイートの一部であり、これには当社の世界中の一つひとつのインターネットのアクセス点におけるCDN、DDoS攻撃からの保護、ABP（Advanced Bot Protection）、およびロードバランシングが含まれます。すべてのコンポーネントが脅威インテリジェンスを共有しているため、リクエストが当社ネットワークに届き次第、最初からエッジでセキュリティとデリバリーロジックを適用することができます。このソリューションは大手SIEMと統合しており、Imperva Attack Analyticsは人工知能（AI）を使って何千ものCloud WAFイベントから明確なナラティブを抽出することで、セキュリティオペレーションセンター（SOC）の効率性を大幅に高めてリスクを低減します。

主要な機能：

- ベストインクラス、PCI認定WAF
- 追加設定なしの自動保護
- 誤検出はゼロに近く、ブロックモードで展開
- Terraformの統合によって、DevOpsの自動プロビジョニングを実現
- 第三者コードの使用によるリスクを低減する、Imperva Research Labsのセキュリティ専門家による裏付け
- セルフサービス式のカスタムルール
- 毎日24時間・週7日のセキュリティオペレーションおよびサポートチーム
- 包括的なクラウドアプリケーションセキュリティおよびデリバリーの一環
- 攻撃分析に関する実用的な洞察となる脅威情報を提供

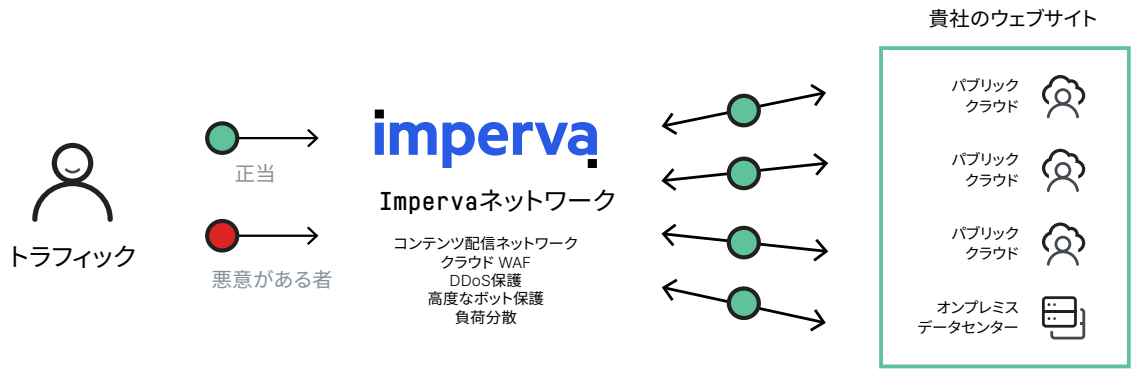

図1：Cloud WAFは一つひとつのリクエストを検査して、悪意のある活動を除去

ウェブ上の脅威から守る

常時稼働する保護機能

高度な識別エンジンは、入ってくるすべてのトラフィックをエッジでリアルタイムにプロファイリングすることで、ウェブアプリケーションに到達するかなり前に正当なクライアントと悪意を持ったクライアントを正確に区別します。この自動セキュリティプロセスでは、ウェブセキュリティの増大、ウェブサーバー使用率の低減、および帯域幅消費の削減のみならず、社内のセキュリティ専門家への依存率の低下、また手動コントロールに伴う精度の低下を減らすことにもつながります。Imperva Cloud WAFの大多数の顧客が、追加設定なしでブロックモードで展開しているのも意外なことではありません。このソリューションでは、ゼロに近い誤検出を通じて正当なトラフィックを入れることが可能だからです。

OWASPの脅威上位10選にとどまらないセキュリティ対策

Imperva Cloud WAFは、クロスサイトスクリプティング、リソースへの不正アクセス、およびリモートファイルインクルージョンなど、OWASPの脅威上位10選から守り、リアルタイムで攻撃を防御します。このソリューションはImperva Application Securityソリューションスタックと合わせて機能することで、DDoS攻撃やSQLインジェクションを活用したAPI攻撃など、異なる攻撃に必要な各種の緩和機能を活用します。

さらに、Imperva Research Labsのチームは新たな脅威を積極的に発見することで、目まぐるしく変わる今日のサイバー攻撃情勢に必要な最新のセキュリティ保護機能を提供します。セキュリティの専門家が新たな脆弱性の開示といった外部の情報源を監視して、第三者コードのリスク低減を支援します。Imperva Research Labsのチームは、クラウドソーシングされたインテリジェンス経由でImpervaに入ってくるすべてのトラフィックを分析して、自動検査を行った後、新たな緩和措置をすべての顧客に伝えます。発見された最新の脅威から防御する新しいセキュリティの署名が毎日追加されます。

使いやすく、簡単に拡張可能

Imperva Cloud WAFは、二要素認証で保護された、使いやすいウェブインターフェースを通じて構成可能です。シンプルなGUIによってカスタムセキュリティ規則を構成できるため、固有の環境内でセキュリティポリシーを最適な形で施行できます。当社のTerraformプロバイダーを通じたDevOpsの自動プロビジョニングによって、何万もの規則の伝搬をわずか数秒で実現できます。高レベルなCloud WAFダッシュボードは、貴社にとっての総合的なセキュリティ脅威情勢の概要を提供します。また、管理はAPIセキュリティ、DDoS攻撃からの保護などと共に一元的に行われます。

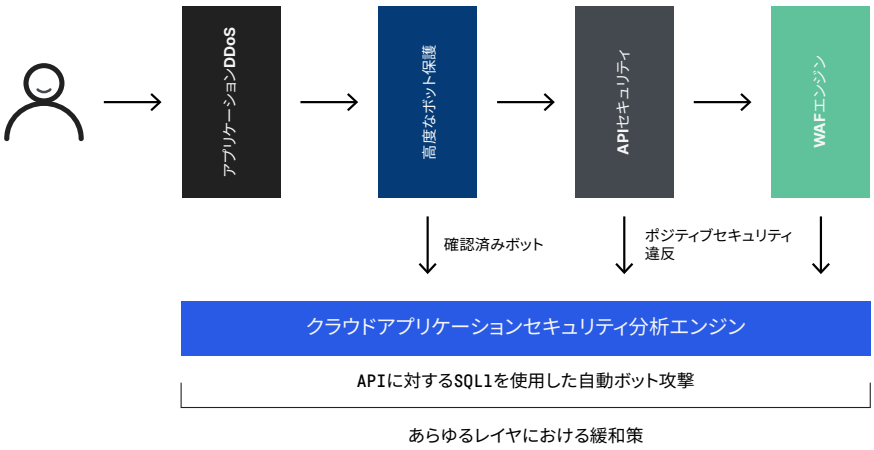

図2：多層防御におけるCloud WAFの役目

IMPERVA APPLICATION SECURITY

Cloud WAFは、顧客体験を最適化すると同時にリスクを削減するImperva Application Securityの主要コンポーネントです。本ソリューションは、以下によってオンプレミスとクラウドのアプリケーションを保護します。

実用的なセキュリティに関する洞察の提供

WAF保護の提供

防御

DDoS攻撃

ボットネット攻撃の軽減

APIを狙ったサイバー攻撃の防止

RASP保護の実行

最適なコンテンツ配信の保証

Imperva Application Securityの詳細については、+1.866.926.4678にお問い合わせいただくか、imperva.comをご覧ください。

Impervaはアナリストが認める**サイバーセキュリティのリーダー企業です。データとアプリケーションがどこにあろうと**セキュリティを保護する取り組みを支援します。