Cloudflare WAF

最新アプリケーションセキュリティのためのWAF

アプリケーションセキュリティの課題

ビジネスにおいてアプリケーションがかつてないほど重要な役割を担うようになりました。攻撃者がひっきりなしに攻撃を仕掛けてくるのにはこうした背景があり、組織的なセキュリティの懸念事項が増える原因となっています。

懸念事項は急増するゼロデイ脆弱性の悪用に対する保護、回避攻撃の検出、アカウント乗っ取りにつながるクレデンシャルスタッフィングのリスクの抑制、データ損失の検出、さらにはアプリケーションへのマルウェアのアップロードのスキャンなど、多岐にわたります。

このような懸念事項は、アプリケーション保護が、より広範で統合されたセキュリティ体制の一部として確立される必要性と並行しています。このセキュリティ体制により保護されるものには、APIの保護、ボットの阻止、クライアント側のリスクの抑制なども含まれます。このすべてが、過度に管理上の手間を増大させるような、チームの負担になることなく実施される必要があります。

Cloudflare WAF

CloudflareのWebアプリケーションファイアウォール（WAF）は、アプリケーションの安全と生産性を維持するCloudflareの高度なアプリケーションセキュリティポートフォリオの要です。セキュリティを完全に可視化したり、OWASP攻撃および急増する脆弱性の悪用に対して階層化された防御を実装したり、さらには、機械学習を使った回避や新しい攻撃の検出、アカウント乗っ取りの阻止、データ損失の防止、さらに多くの機能を持ち、その一方でより広範なエンタープライズセキュリティワークフローに簡単に組み込むことができるのは、Cloudflare WAFのみです。APIセキュリティやボット管理などのパワフルなアプリケーションセキュリティ機能は、Cloudflare WAFに完全に統合され、世界有数の広範なグローバルクラウドプラットフォームから得られるパワフルなルールエンジンで使用されます。

攻撃の可視化と検出

Cloudflareでは軽減の有無にかかわらず、すべてのトラフィックを可視化するために、さまざまなセキュリティ分析を実施しています。セキュリティチームはそこから未知の攻撃、対応すべき保護を知ることができます。WAFの攻撃スコア、ボットスコア、コンテンツのスキャン分析が明らかになります。

急増する攻撃を迅速に保護

年に何千件、何万件と見つかる脆弱性に対し、CloudflareのWAFは新たに発見された（ゼロデイの）脆弱性の悪用を阻止するための新たなマネージドルールを迅速に追加しています。Cloudflareのマネージドルールは、回避の検出に機械学習を用いたWAF攻撃スコアで補足されたデータで脆弱性の悪用を阻止します。

OWASPの脅威上位10件

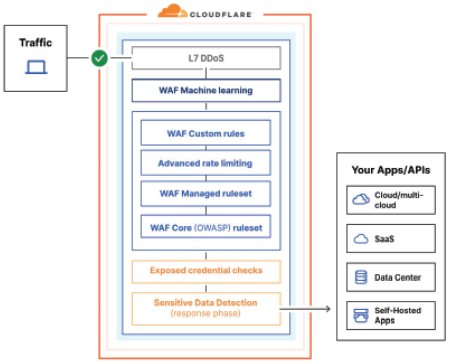
攻撃には、OWASPの脅威上位10件をまとめたリストに含まれる既知の攻撃タイプなど、階層化された防御が必要です。CloudflareのOWASPコアルールセットは常時更新され、脅威スコアを計算し、そのスコアを基準にアクションを実行する1つのエンティティとして機能するよう設計されています。このルールセットはリスクとセキュリティの要件に応じて設定できます。

Cloudflare Webアプリケーションファイアウォールを選ぶ理由

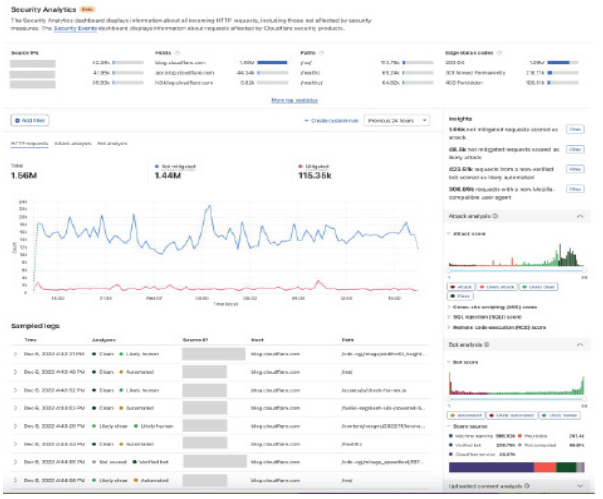
- **Cloudflareの保護はより効率的。**Cloudflareでは階層化された保護とともに、より効率的なWAFセキュリティを提供します。
  - セキュリティ分析
  - 複数のマネージドルールセット
  - カスタムルール
  - 機械学習による検出
  - 機密データの検出
  - 資格情報の盗難チェック
  - 高度レート制限
  - マルウェアのアップロードのスキャン

- **Cloudflareの対応は迅速。**Cloudflareはより迅速に脆弱性の悪用を防御します。Log4jのような主要な脆弱性では、他のWAFベンダーより1営業日早く複数のマネージドルールを公開しました。

- **Cloudflareのアプリケーションセキュリティは総合的。**CloudflareのWAFは、APIセキュリティやボット管理などを含め、アプリケーションセキュリティポートフォリオ全体に統合されており、さらに、世界有数の広範なグローバルクラウドプラットフォームと直結しています。



WAFセキュリティ分析



エンタープライズセキュリティに対応したWAF

SIEM統合、SOC対応

Cloudflare APIと未加工ログの統合により、お客様のSIEMと統合しやすくなり、Cloudflareが提供するインテリジェンスでお客様のセキュリティオペレーションセンター（SOC）を強化することも容易になります。

DevSecOpsが容易に

すぐ利用可能なTerraform統合により、アプリケーションセキュリティをDevOpsのアプローチの一環に組み入れることができます。

Cloudforce Oneを活用

Cloudflareのアプリケーションセキュリティでは、脅威対応チーム「Cloudforce One」から脅威インテリジェンスを受け取り、急増するインテリジェンスとTTPがベースとなった新しい検出情報をもとに脅威をブロックします。

Cloudflareのリーダーシップ

企業は、Cloudflareのグローバルネットワークを企業セキュリティの境界にすることによって、有効性の高いアプリケーションセキュリティ体制を実現できます。Cloudflareのアプリケーションセキュリティポートフォリオは、その強度と幅広さが評価され、数々の栄誉に輝いています。GartnerがCloudflarを2022年の『Gartner® Magic Quadrant™ for Web Application and API Protection（WAAP）』でリーダーに選出。『The Forrester Wave™ for WAF』でCloudflareがリーダーに選出。GartnerはCloudflare WAFを2022年の「カスタマーズチョイス」にも認定しました。Frost & Sullivanが2020年の「Global Holistic Web Protection」でCloudflareをイノベーションリーダーに選出、さらに、IDCおよびForresterがCloudflareを2021年のDDoSリーダーに認定しました。

Webアプリケーションのセキュリティ	
複数のWAFルールセットで多層防御	複数のルールセットで、あらゆるリクエストコンポーネントの悪意あるペイロードを阻止： 1. Cloudflareマネージドルール 2. OWASPコアルールセット 3. すべての攻撃を阻止するカスタムルールセット 膨大な量のトラフィックでテストし、誤検知を最小限に抑えた新マネージドルール。
ルールの更新によりゼロデイ攻撃から保護	Cloudflareのセキュリティチームが絶えず更新し、新手の攻撃やゼロデイの脆弱性悪用に対しても、パッチやアップデートの提供前に保護するルール。
機械学習による検出	階層化ルールセットを補完する機械学習モデルによりバイパス試行を阻止します。ルールには4つの異なる攻撃スコア（総合WAF攻撃スコア、XSS攻撃スコア、SQLi攻撃スコア、RCE攻撃スコア）が利用できます。
主要なCMSおよびEコマースプラットフォーム向けのプラットフォーム固有のルールセット	WordPress、Joomla、Plone、Drupal、Magneto、IISなどのプラットフォームを追加設定なしで保護できます。追加料金はかかりません。
カスタムルールの設定	ルールやルールセットをデプロイする際は、ALLOW、BLOCK、MANAGED CHALLENGE、JS CHALLENGE、SKIP、LOG、LEGACY CAPTCHA、CUSTOM RESPONSESから選択可能。
高度レート制限	アプリケーションやAPIを標的とした不正利用、DDoS攻撃、ブルートフォース攻撃の試みを、各IPのレート制限や、ヘッダー属性（つまり、キー、Cookie、トークン）、ASN、または国の指定によって阻止します。
脅威インテリジェンスフィード	既知のオープンSOCKSプロキシ、VPN、ボットネット、コマンドサーバーおよびコントロールサーバー、マルウェアソース、アノニマイザーのIPからの接続を阻止します。
機密データの検出	個人を特定できる情報、財務情報、クレジットカード番号といった機密データや、APIキーのような秘密を含む応答を検出します。
資格情報の流出チェック	盗まれた資格情報を使ったブルートフォース攻撃を、エンドユーザーのアカウントが乗っ取られる前に検出します。
コンテンツアップロードのスキャン	WAFコンテンツスキャニングが、アップロードされたファイルをスキャンし、マルウェアの存在を確認。軽減はWAFのカスタムツールで実施。
SSL/TLS	お客様のアプリケーションへのSSLトラフィックを、完全にオフロードし、構成します。
誤検知の減少	新ルールは膨大な量のトラフィックでテストし、誤検知を最小限に抑えるようにしています。
gRPCとWebSocketのサポート	gRPCとWebSocketのエンドポイントへのトラフィックをプロキシし、安全にします。
カスタマイズ可能なブロックページ	訪問者に関する適切な詳細指定で、ブロックページをカスタマイズします。
広範なCloudflare製品スイートとの完全な統合	アプリケーションパフォーマンス、地理的ルートトラフィック、エッジコンピューティングの活用を向上させます。

可視化、レポート作成、プログラム作成	
セキュリティ分析	機械学習によるスコアをもとに、すべての潜在的攻撃を可視化
リアルタイムロギングと未加工ログファイルのアクセス	可視性を高めてWAFの微調整を可能にします。すべてのWAFリクエストを対象に、詳細な分析を行います。
ペイロードロギング	インシデント解析のための悪意のあるペイロードのログ取得と暗号化を行います。
SIEM統合	既存の SIEM に対して直接ログをプッシュまたはプルします。
Terraformで統合	アプリケーションセキュリティをCI/CDワークフローに組み込みます。
管理	
単一コンソールで管理	管理を簡素化し、単一コンソールでグローバルなアプリケーションセキュリティとパフォーマンスをデプロイし、管理できます。
アカウントレベルの管理	全ドメインについてアカウントレベルのWAF設定を一度行うだけで、WAF管理の時間を節約できます。
SLAを使用した高稼働率	稼働率100%保証。SLA違反には違約金が発生します。
ハードウェア、ソフトウェア、調整が不要	DNSを少し変更するだけでデプロイできます。
PCI認定	Cloudflareはレベル1サービスプロバイダー認定を受けています。
FedRAMP認証取得済み	アプリケーションセキュリティを含めた当社のCloudflare for Government スイートは、FedRAMP準拠の認証を取得しています。