CLOUDFLARE

製品概要

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はそのためで、攻撃対象領域が拡大しています。

懸念される課題は、急増するゼロデー脆弱性の悪用に対する常時保護、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低減、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アップロードのスキャンなど、多岐にわたります。

加えて、アプリケーション保護をはじめ、APIの保護、ボットの阻止、クライアントサイドのリスク低減も含めたより広範で統合されたセキュリティポスチャを確立する必要もあります。これらすべてを、管理するチームに過度の負担を強いることなく実現しなければなりません。

Cloudflare WAF

Cloudflare Web Application Firewall（WAF）は、アプリケーションの安全と生産性を維持する当社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。セキュリティの完全可視化、OWASP攻撃や新手の脆弱性悪用に対する階層型保護、機械学習を活用した回避や新型攻撃の検出、アカウント乗っ取りの阻止、データ損失の検出などの機能を備え、ホスト場所にかかわらずアプリケーションを保護できるのは、Cloudflare WAFだけです。APIセキュリティやボット軽減などの強力なアプリケーションセキュリティ機能は、Cloudflare WAFに完全統合され、同一のパワフルなルールエンジンを呼び出します。そして、すべて世界初のコネクティビティクラウドから提供されます。

攻撃の可視化とシンプルなオンボーディング

Cloudflareは、当社ならではのセキュリティ分析で、軽減するしないにかかわらずあらゆるトラフィックを可視化します。脅威状況を即座に可視化することで投資収益の具体的把握が可能になるため、オンボーディング後すぐに、攻撃トラフィックと作成するべき保護を理解できます。

急増する攻撃を迅速に保護

1年に何万件もの脆弱性が見つかる中、CloudflareのWAFは、新たに発見された（ゼロデーの）脆弱性の悪用を阻止する新たなマネージドルールを迅速に追加しています。Cloudflareは、マネージドルールとそれを補完するWAF攻撃スコア（機械学習に基づく）で脆弱性の悪用を阻止し、回避を検出します。

大規模グローバルネットワークに支えられた脅威インテリジェンス

セキュリティが効果を発揮するには、まず最高品質のデータが必要です。当社の広大なグローバルネットワークはインターネットの20%をプロキシしており、脅威状況に関する比類ないインサイトを提供します。このデータは機械学習モデルの強化にもつながります。当社では、機械学習と従来のシグネチャベースの検出手法を併用して攻撃の試みを高精度で検出し、軽減しています。

アプリケーションセキュリティの課題

Cloudflareは、より効果的に保護します。

階層型の保護により、効果の高いWAFセキュリティを提供します。

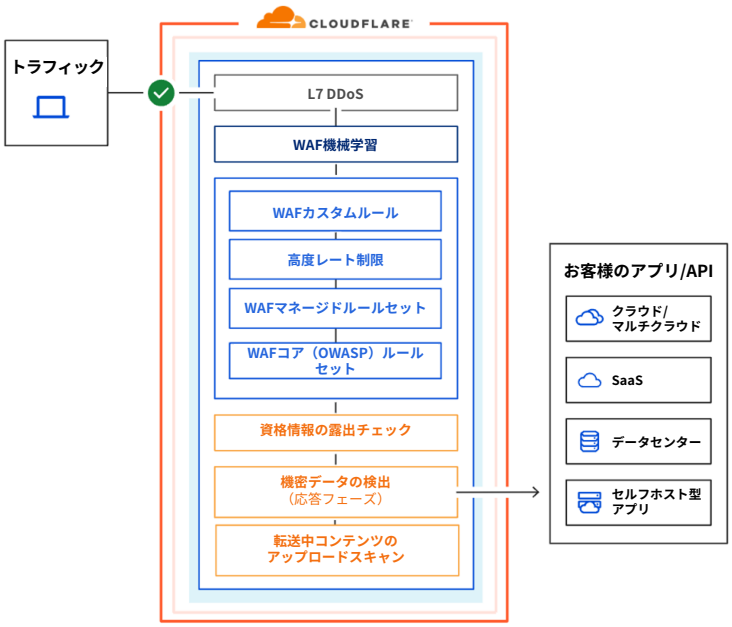
- セキュリティ分析
- 複数のマネージドルールセット
- カスタムルール
- 機械学習による検出
- 機密データの検出
- 資格情報の盗難チェック
- 高度レート制限
- アンチマルウェアアップロードスキャン

Cloudflareは、より迅速に対応します。

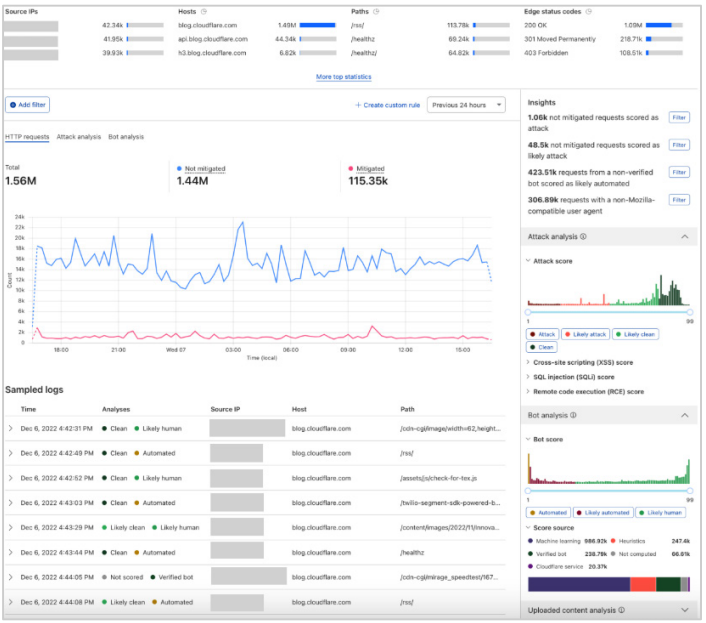
より迅速に脆弱性の悪用から保護します。HTTP/2 Rapid Reset、Log4jといった多数の重度脆弱性に関しても、当社はマネージドルールを他のWAFベンダーよりも1営業日早く適用しています。

Cloudflareは、アプリケーションセキュリティを完全に統合しています。

WAFは、API GatewayやBot managementをはじめ、当社のアプリケーションセキュリティポートフォリオの他の機能と完全に統合され、それらすべてがCloudflareのコネクティビティクラウドからシングルパスで提供されます。



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、SIEMと統合しやすく、Cloudflareが提供するインテリジェンスで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です。

DevSecOpsが容易に

設定要らずのTerraform統合で、アプリケーションセキュリティをDevOpsのアプローチに自然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は、当社の脅威対策チーム「Cloudforce One」から脅威インテリジェンスを受け取り、最新インテリジェンスとTTPに基づく新たな検出によって脅威をブロックします。

Webアプリケーションの保護	
複数のWAFルールセットで階層型の保護	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します： 1. Cloudflareマネージドルール 2. OWASPコアルールセット 3. あらゆる攻撃を阻止するカスタムルール 新たなマネージドルールは膨大な量のトラフィックでテストし、偽陽性を最小限に抑えます。
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ー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します。
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、次のアクションを使用して、ポジティブまたはネガティブのセキュリティモデルを作成します：BLOCK、MANAGED CHALLENGE、JS CHALLENGE、SKIP、LOG、LEGACY CAPTCHA、CUSTOM RESPONSES。
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（キー、Cookie、トークンなど）、自律システム番号、または国の指定によって阻止します。
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。
資格情報の露出チェック	盗まれた資格情報を使ったクレデンシャルスタッフィング攻撃を、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 Content Scanningは、アップロードされたファイルをスキャンし、マルウェアを検出します。カスタムルールを作成することで、そのシグナルをリクエストの他のパラメータと組み合わせることができます。
SSL/TLS	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。
偽陽性の削減	新ルールは膨大な量のトラフィックでテストし、偽陽性を最小限に抑えます。
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	Web訪問者のために適切な詳細情報を盛り込んで、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の向上、トラフィックの位置情報ルーティング、エッジコンピューティングの活用を実現します。

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します。
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に、悪意のあるペイロードをログに記録し、暗号化します。
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。
高可用性（SLA締結）	稼働率100%保証。SLA違反には違約金が発生します。
ハードウェア不要、ソフトウェア不要、調整不要	DNSを少し変更するだけでデプロイできます。
PCI準拠認定	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の認証を取得しています。

さらに詳しい情報をご覧になりたいですか？アプリケーションセキュリティデモシリーズにご登録ください。