Web アプリケーション ファイアウォールの 5 つの迷信を払拭

ミッションクリティカルな業務をオンラインで行う組織にとって、Web アプリケーションファイアウォール（WAF）は、悪性トラフィックを排除し、正当なトラフィックの通過を許可する防御の最前線である必要があります。WAF テクノロジーは長年利用されてきましたが、WAF の当初の定義はあまりにも単純すぎ、進化した現代の用途にふさわしくありません。このため、多くのビジネスリーダーやセキュリティ担当者は、時代遅れの認識や迷信から抜け出せずにいます。

こうした迷信のせいで、組織のスタックにすでに存在しているであろう WAF の能力が過小評価され、十分に活用されず、その結果、攻撃者の侵入を許し、運用上のリスクを高めている可能性があります。WAF テクノロジーの包括的なデジタルセキュリティに対するニーズは拡大し続けています。セキュリティ対策を改善し、最新の WAF テクノロジーの保護機能を活用するためには、まず、最も一般的な迷信に対処する必要があります。

2023 年第 3 四半期には、99 億 3,000 万件の Web アプリケーション攻撃を確認

2023 年第 3 四半期の 1 日当たりの攻撃数は、ピーク時に約 3 億 2,700万件

出典：Akamai の脅威リサーチ

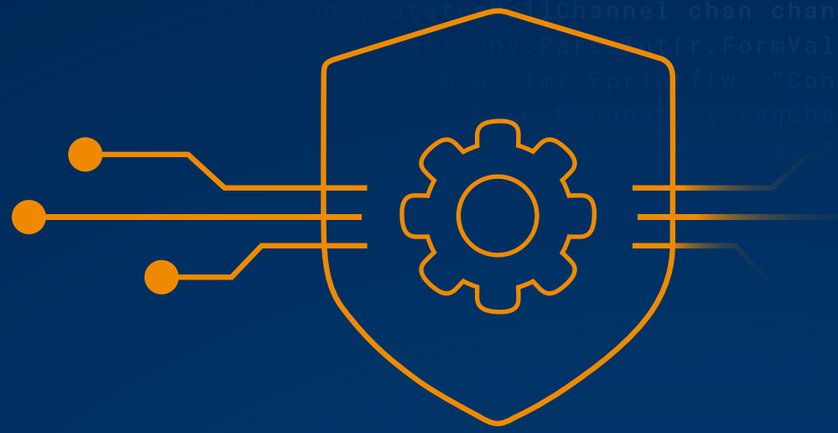
迷信 1

WAF の効果を保つためには手動での定期更新が必要

最新の更新から最新の保護が提供されるのは確かですが、この迷信には誤解がいくつかあります。現在、多くの組織で、WAF ルールの継続的な更新や調整に必要なリソースやセキュリティ専門知識が不足しています。自動化された適応型の更新は、時間の節約や利便性だけでなく、リスクの軽減というメリットも企業にもたらします。手動更新を選択した企業を調査したところ、77% 以上で、ルールセットの更新に 5 バージョン以上の遅れが見られました。Akamai は継続的かつ自動的に WAF の更新をプッシュします。これが、組織における時間や、リソースへの投資、不要なリスクの削減につながります。

迷信 2

WAF はトラフィックに対してゲートを開閉するだけ



従来の WAF は、ユーザーと Web アプリケーションをつなぐトラフィックの中央に配置され、定義されたルールのリストに沿って HTTP トラフィックを検査していました。Akamai のソリューションは、従来の WAF の枠を超えて迅速かつ大胆に革新され、DDoS **緩和**、API セキュリティ、ボット緩和、マルウェア検知、機微な情報の探索、パフォーマンス高速化など、さまざまな機能を備え、防御を強化します。また、App & API Protector のリリースに伴い、Site Shield、mPulse Lite、EdgeWorkers、Image & Video Manager、API Acceleration など、さらに多くの人気テクノロジーが WAF セキュリティソリューションにまとめられるようになりました。Akamai の WAF ソリューションは、セキュリティエキスパートが複数の資産にわたるセキュリティ保護を完全に可視化し、制御できる多機能テクノロジーと言えます。

迷信 3

WAF がセキュリティ担当者のアラート疲れを助長

最前線で防御しているセキュリティチームに質問してみてください。そうすれば、調査する必要のある膨大なアラートやトリガー（特に WAF 防御によって生成されたもの）によって、いかに疲弊し、圧倒されているかわかると思います。Akamai が当社の WAF ソリューションを強化するコアテクノロジーである Adaptive Security Engine を開発したのは、まさにこの問題を解決するためです。Adaptive Security Engine により、機械学習、リアルタイムのセキュリティインテリジェンス、高度な自動化、400 人を超える Akamai の脅威リサーチャーからの知見を組み合わせ、最新の保護を実現できます。Adaptive Security Engine は、Web アプリケーションと API の資産全体を保護するように構築されています。他のソリューションとは異なり、各顧客に固有のトラフィックや攻撃のパターンを学習し、各リクエストの特性をリアルタイムで分析して、その知識を将来の脅威の傍受や適応に利用します。セキュリティチームは、Adaptive Security Engine を使用することで、アラート疲れを回避できるだけでなく、貴重な時間を節約し、負担を軽減しつつ、アプリケーションや API を保護し続けることができます。

Adaptive Security Engine の推奨チューニングにより減少した、フォールス・ポジティブ（誤検知）の比率

5 倍

迷信 4

カスタマイズ性の高い WAF ルールほどセキュリティが強化される

ルールが増えるほど、セットアップやテスト、分析の回数も増えます。ルールの数を増やしても減らしてもセキュリティの向上には関係ありませんが、多ければ多いほど良いと信じるセキュリティエキスパートでも、心配する必要はありません。Akamai の WAF には、無制限のカスタムルールが用意されています。また、当社では事前に対応する適応型のルール更新を採用していますが、これもルールの数に関係なく配信されます。セキュリティチームは、自動更新と自動セルフチューニングを通じ、デジタル資産全体の WAF 設定を効率的かつ効果的に検証できます。新しいルールを追加したい場合は、評価モードを使用すると、新しいルールや変更されたルールによるライブトラフィックへの影響を評価でき、カスタマーポータルのダッシュボードでリアルタイムの効果を確認できます。このシャドーモード形式のテストにより、新しいルールが導入環境で期待どおりの保護効果を発揮します。

迷信 5

WAF は開発者の妨げになるのみ

開発者は、現代の組織にとって、顧客に認められる価値を生み出す原動力です。セキュリティが妨げられると、技術革新が鈍化し、リリースサイクルに遅延が発生して、価値実現までに時間がかかるようになります。その一方で、テストせずにリリースすると、事業運営が滞るような、セキュリティ面の壊滅的な結果がもたらされる可能性があります。Akamai は、セキュリティのエキスパートや開発者を支援します。アプリや API などを保護する WAF 防御により、DevSecOps の文化でスピードやアジリティ、コラボレーションを促進できると確信しています。そのため、当社の WAF 機能はすべて、オープンな AppSec API または Terraform を介して管理できます。これにより、担当チームはアプリケーションや API のオンボーディングのほか、セキュリティ設定の管理も自動化できます。さらなるサポートが必要な場合は、Akamai TechDocs で提供している、開発者のために特別に設計された最新のインタラクティブで直感的な機能を利用できます。

Akamai が提供するサポート

アタックサーフェスが拡大し、脅威が絶えず進化している上、攻撃者のモチベーションは高まるばかりです。このような状況から、防御側には従来の WAF 防御を超える可視性が必要です。Akamai App & API Protector は、Web アプリケーションファイアウォール、ボット緩和、API セキュリティ、DDoS 防御など、多くのセキュリティテクノロジーを 1 つにまとめたソリューションです。カスタマイズされた推奨ポリシーをワンクリックで実装でき、それだけでセキュリティ保護が継続的かつ自動的に更新されます。また、コアテクノロジーである Adaptive Security Engine は、機械学習、リアルタイムのセキュリティインテリジェンス、高度な自動化、400 人を超える脅威リサーチャーからの知見を組み合わせ、最新の保護を実現します。

無料トライアルをぜひご利用ください。また、貴社の最も重要な Web 接続アセットを保護し、リスクと運用上のフリクションを軽減するための Akamai の取り組みもご確認ください。