Web Application Firewall の選択に関する 10 の誤った通念

ウェブアプリケーションのセキュリティ確保は骨の折れる作業で、特に専任のセキュリティスタッフがいない場合やトレーニングを実施していない場合はきわめて困難です。Web Application Firewall（WAF）には、アプリケーションのパフォーマンスを維持しながら脅威を防ぐ性能が求められます。しかし、WAF ソリューションは多数あり、その選定は容易ではありません。このドキュメントでは、まず WAF にまつわる誤った通念を払拭し、その選定において最も重視すべき 10 の評価ポイントを挙げました。攻撃を懸念することなくビジネスの成長に心おきなく集中できるようになりましょう。

誤った通念その 1：WAF の運用は複雑

そんな WAF ばかりではありません。Akamai WAF では、管理が簡単なルールセットを使用して、分散型サービス妨害（DDoS）とアプリケーションレイヤーのセキュリティをシンプルにします。この WAF ルールは、最新のサイバーセキュリティ脅威からの保護に対応して自動的に更新されるため、防御対策が常に最新の状態に保たれます。脅威を阻止しつつ正規ユーザーのアクセスを許可するよう、ルールは徹底的にテストされているので安心して利用できます。さらに、セキュリティの専門知識が必要な場合は、Akamai が 24 時間／ 365 日体制でサポートを提供します。

誤った通念その 2：カスタマイズ可能なルールが多いほどセキュリティが強化される

ルールが少ないほど、使いやすさは向上します。カスタマイズするルールが増えると、必要以上に複雑になり、特にルール同士の依存関係や同期した動作の詳細を深掘りする必要が出てきます。それを判断できるセキュリティの専門知識を備えたスタッフが組織にいない場合は管理が難しくなります。Akamai の自動化された WAF ルールセットは、8 つのカテゴリーにまとめられているので、必要な作業はそれらを有効にすることだけです。調整する項目が少ないので、あなたが微調整することで問題が発生する可能性は低くなります。

誤った通念その 3：サービス停止はビジネスにつきもののコスト

サービス停止は、オンラインでビジネスを行う上で、もはや容認できるコストではなくなっています。Network World の報告によると、1 時間のダウンタイムによる損失は、小規模企業の場合は最大 8,000 ドル、中規模企業では最大 74,000 ドルにのぼる可能性があります。世界 130 か国以上、1,700 以上のネットワークで 100% の可用性を備えた規模と耐障害性を提供する Akamai は、世界の FinTech 企業トップ 8 社および米国のインターネット小売企業トップ 91 社を含め、可用性を最も重視する業界で信頼されています。

誤った通念その 4：WAF ルールのリリースが早いほど速やかにアプリケーションを保護できる

WAF ルールが適切に検証されたうえで公開されなければ、問題が生じます。検証が十分でない WAF ルールを本稼働環境の Web サイトに適用すると誤検知が発生して逆効果になることがあります。Akamai では新しいルールのリリース前に 2 段階でテストします。まず、ラボで既知の正当なトラフィックと悪意のあるトラフィックに対してテストを実施し、次に、Akamai のプラットフォーム上で実際のインターネットのトラフィックに照らして誤検知と検知漏れが起きないかを十分に分析します。スピードを重視するあまり、品質をおろそかにして、ビジネスの場を実験台にすることがあってはなりません。

誤った通念その 5：クラウドのデータを利用した脅威分析のみで保護対策は十分である

クラウドで収集したデータに依存する分析のみでは、精度、妥当性とそのふるまいのコンテキストが十分得られません。また、そのような分析では、誤検知（フォールスポジティブ）は考慮されていません。6,000 社を超える大規模なオンライン企業の数十億台のデバイスに 95 エクサバイト以上のデータを配信している Akamai は、各産業界および世界中の莫大な量のトラフィックを正当なものも、悪意あるものも把握しています。トラフィックを Akamai のセキュリティ専門家が観察することで、攻撃および正当なトラフィックの変化を把握しています。このような知見は、すべての業界に渡る防御ルールの精度向上に役立てられています。

誤った通念その 6：ルールのトリガー（通知）の数が多いほど良い成果が得られる

多すぎるルールトリガーの通知数は、機械が発するノイズでしかありません。本当に重要なのは、WAF が検知した数々の攻撃の相関分析とスコアリングによって得られる誤検知を減じた攻撃検知のしくみです。Akamai は、その配信サービスにおいて毎日 2 兆を超えるインターネットのやり取りと、1 億個以上の IP アドレスを取り扱っているため、他社にはないインテリジェンスと知見を得ることができます。攻撃の多くは、1 つの業界を起点に、他の業界へも広まっていきます。毎週、複数の業界を横断して数億件のウェブ攻撃が確認されていますが、Akamai では独自の視点により、脅威に先手を打ち、サイバー攻撃からお客様を保護します。

誤った通念その 7：API は保護しなくてもよい

かつてないほど相互のつながりが増えているデジタルの世界では、ウェブページを保護するだけでは不十分です。API のセキュリティを適切に保護することで、アタックサーフェス（攻撃の対象となり得る領域）を減じることができます。Akamai WAF は、IP アドレス、位置情報、異常なアクセス、過剰なリクエストレートに基づいて API 形式で行われる攻撃トラフィックをブロックし、DDoS 攻撃やウェブアプリケーション攻撃から API を保護します。また、悪意のあるコンテンツの API リクエスト（JSON と XML を含む）を自動的に検査し、単純な Web サイトから API を扱うアプリケーションサーバーまで高度な保護を拡張します。

誤った通念その 8：WAF はすべてのゼロデイ攻撃を防ぐことができる

ゼロデイ攻撃は、その名が示すとおり既知の攻撃ではなく、防御を確約できるベンダーはいません。とは言え、WAF では防御できないという意味ではありません。たとえば、Akamai WAF はアノーマリベースのルールを使用して、既知のケースとの類似するゼロデイ攻撃を検知します。アノーマリ・スコアリング・メカニズムに基づき設計された Akamai WAF は、追加のチューニングを必要とせずとも、ゼロデイ脆弱性を悪用する攻撃をこれまでも検知してきました。また、Akamai WAF のルールは自動的に更新されるため、絶えず変化する脅威の現状を常に把握しつづける負担はありません。

誤った通念その 9：WAF はボットをすべて緩和できる

一般的な WAF はボットに対しても、いくつかの重要な保護レイヤを提供します。Akamai WAF は、既知のボットだけでなく、一度に大量のリクエストを送信する未知ボットもブロックします。人間が介することなく高頻度のアクセスを繰り返すボットによってシステムがダウンすると、正当なトラフィックも影響を受けます。WAF のしくみを使用すれば、リソースを奪うボットの流量を管理でき、他に悪影響が及ばないようにすることができます。より巧妙なボットを作り出す攻撃者に組織が標的にされた場合、WAF を回避する方法を見つけてしまう可能性もあります。そのような場合のために、Akamai は不正ログインなどを行う高度なボットの脅威を検知して防御する、より進んだボット管理ソリューションも提供しています。

誤った通念その 10：ポイントソリューションはそれぞれの専門分野では優れている

最新のサイバーセキュリティの脅威から保護するには、さまざまなセキュリティ製品やサービスで記録された大量のインシデントデータから得られた知見を応用することで、保護の自動化がより効果的に、アノーマリ検知がより高性能に、そしてルールセットもより高品質になります。複数のベンダーのポイントソリューションを組み合わせて使用するセキュリティ戦略は、往々にして管理が難しく、その扱いのトレーニングがより多く必要となり、それらの統合に関しても課題が発生しがちです。

アプリケーションレイヤーと DDoS 防御により、セキュリティ対策をより身近なものにする
Akamai WAF について詳しくは、Akamai.com/Security をご覧ください。

Akamai