Akamai

ホワイトペーパー

Web アプリケーションセキュリティのシンプル化

Web アプリケーション攻撃

最新の Web アプリケーションは、特にマイクロサービスベースのアーキテクチャの導入が増加しているため、複雑になっています。オンラインでのやり取りのほぼすべてが API に大きく依存していることも、この複雑さに拍車をかけており、ハッカーにとっての新しいエントリーポイントになる可能性があります。一方で、既知の Web の脆弱性は残り続けるため、新しい世代のコード作成者がその脆弱性をアプリケーションに引き継いでしまいます。今日の攻撃者は、これにつけ込もうと手口を巧妙化させており、Web アプリケーションや API だけでなくクライアント側の脆弱性まで標的にして、ボット、DDoS 攻撃請負サービスを活用し、マルチベクトル攻撃を仕掛けるようになっています。

しかし今までどおり、何かに乗じて仕掛けるのが最も一般的な Web 攻撃です。特定の組織を標的にするのではなく、脆弱性を発見した組織に攻撃を仕掛けます。スキャナーは自動化されたボットを使用して、Web サイトをランダムにクロールし、何千もの脆弱性を常に探しています。脆弱性が発見されると、攻撃者によってデータベース内の機密情報が漏洩されたり、悪性のファイルが Web サーバーにロードされたり、莫大な量のトラフィックでサイトが攻撃されたりする可能性があります。

Web 攻撃に伴うリスクとは

リスク許容度の低い組織には、内部（システム、サプライチェーン、運用など）と外部（パートナー、顧客、管轄機関など）の両方で、相互に信頼の絆を作るための高度なセキュリティ成果が必要です。特に、マイクロサービスアプリケーションのパーツ間のシンプルな内部フローから、企業間の大規模なやり取りに至るまで、API のセキュリティを確保することが重要です。API は、さまざまなシステムやパートナーエコシステムの間をつなぎ、デジタルおよびオムニチャネルの顧客体験を実現するデジタルグルー（接着剤）として機能するからです。

しかし、サイバー犯罪者は、甚大な損害を与えるように設計された Web 攻撃手法をほぼ無限に持っています。ハッキングが成功して機微な情報が流出したり、DDoS 攻撃を受けてサイトが利用できなくなったりすると、この信頼関係が崩れ、顧客ロイヤルティの喪失、規制に基づく罰金、訴訟、ブランドの評判の低下により、大きな損害を被る可能性があります。

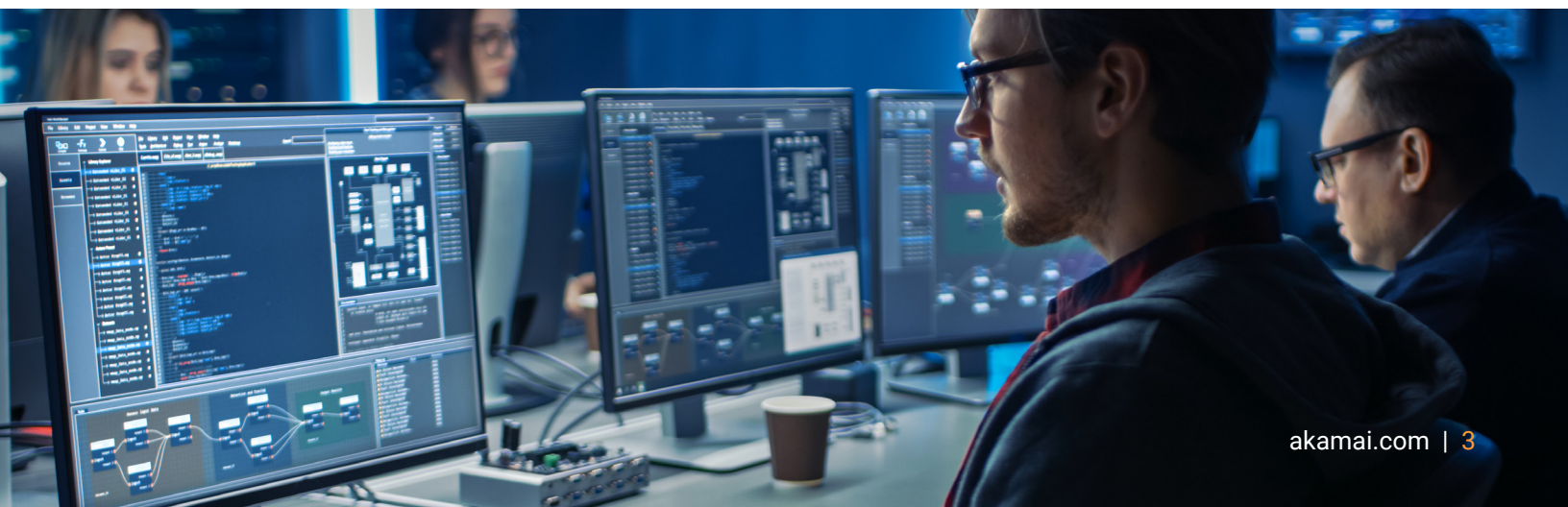
Web アプリケーションセキュリティに関する課題

クラウドベースの Web アプリケーションと API 保護（WAAP）ソリューションは、さまざまな形態の Web アプリケーション攻撃、DDoS 攻撃、API ベースの攻撃を緩和するように設計されています。しかし、ファイアウォールの主な課題の 1 つは、アプリケーションの変更、脅威の進化、アップデートが発生するたびに AppSec チームが常にルールを分析し、調整しなければならないことです。スキルの高い人材は 2 年程度で配置転換されるケースが多く、経験豊富なセキュリティ専門家の確保は依然として課題となっています。こうした業務は、多くの場合、熟練したオペレーターを必要とする時間のかかる手動プロセスであり、人材の異動、学習ライフサイクル、専門的なテクノロジー統合アーキテクチャといった理由から、ほとんどの組織にとってスケーラビリティがありません。

大量のアラートを見ているうちに疲労がたまり、実際の攻撃とフォールス・ポジティブ（誤検知）を正確に区別する能力が大幅に低下するにつれて、すぐに古くなるセキュリティポリシーが、フラストレーションのもとになりかねません。ルールを効果的に調整する能力がセキュリティチームにない場合も、正当なユーザーへの影響やビジネスの中断を避けようとして、本来あるべき保護を外し、ついついリスクの高い状態を受け入れてしまう傾向があります。

Akamai WAAP を選ぶ理由

Akamai App & API Protector は、ボットの可視化や緩和などを行うクラウドベースの WAAP ソリューションです。ネットワーク／アプリケーションレイヤーに対するさまざまな脅威からアプリケーションと API を大規模に保護するように設計されており、労力もオーバーヘッドも軽減します。Akamai のセルフサービス型オンボーディングウィザードによって事前に知識を習得しておく手間が減り、ユーザーはガイダンスと知見を活用しながら迅速かつ容易に資産のセキュリティを確保できます。当社の自動セットアッププロセスでは、セキュリティトリガーの分析とアプリケーションのふるまいの学習を通じて保護を自動調整し、リソースのさらなる節約を実現します。App & API Protector は、組織内の摩擦、運用上の負荷、導入時の障害の原因となっている、ファイアウォールが現在抱える問題の多くを解消するのです。



Akamai によって完全に管理できる自動保護機能は、世界で最も分散されたプラットフォームで実施され、アプリケーションセキュリティと API 保護の作業が自動化されます。SQL インジェクション、クロスサイトスクリプティング、ローカル・ファイル・インクルージョンなどの Web 攻撃から自動的に保護する機能は、広範囲をカバーし、継続的なメンテナンスは実質的に不要になります。また、機械学習とヒューリスティックを適用することで、一般的なネットワーク全体のチェックではなく、ポリシーごとにトラフィックから誤検知パターンを特定する機能が強化され、関連性と実用性の高い結果を得ることができます。

CVE ごとに詳細な情報（脅威レベルや、Akamai の現在の保護に関する知見など）を提供する CVE ルックアップツールを使用すれば、セキュリティ状況を検証し、社内のセキュリティおよび開発戦略の指針として活用できます。さらに、コードとしての Akamai、API、CLI、Terraform、および統合を含む、標準搭載された Akamai の SecDevOps 統合により、社内の連携強化や市場投入までの時間短縮を実現します。

適応型防御でレベルアップ

では、Akamai App & API Protector はどのようにシンプルさと正確さの両方を実現しているのでしょうか。最初にお伝えしたいのは、App & API Protector の中核テクノロジーである Akamai Adaptive Security Engine の独自性です。顧客ごとにトラフィックと攻撃パターンを学習し、すべてのリクエストの特性をリアルタイムに分析して、その知識を将来の脅威の傍受や適応に利用します。このテクノロジーは、異常な、または不審なすべてのデータポイントを考慮し、リクエストごとに脅威スコアを割り当てることで、セキュリティ運用の負担を軽減します。脅威スコアが高いほど防御が強化されます。検知された脅威のレベルに応じて保護を動的に変更できるため、フォールス・ポジティブ（誤検知）のレベルを極めて低く抑えながら、巧妙にセキュリティをすり抜けようとする攻撃を特定することができます。

アプリケーション攻撃においては、通常、何らかの形で偵察活動が行われますが、攻撃者が脆弱性をスキャンすると、Akamai はどのような技法と方法が使用されたかのデータを残します。これにより、迅速な特定だけでなく、再度の攻撃に備えて特定のトラフィックパターンを照合するためのデータを得ることができます。攻撃者が頻繁に攻撃を試みるほど、保護が強化されるのです。

Akamai の調査によると

7 億 8,000 万件以上
の Web アプリケーション攻撃
アラートが毎日発生

260 億件以上
のボットリクエスト

932 TB 以上
のデータを毎日分析

クラウドソーシングの脅威インテリジェンス

インターネット上で最も攻撃されている Web サイトの多くは、Akamai のお客様のサイトです。その中には、小売企業上位 10 社のうち 9 社、銀行の上位 10 行すべて、ヘルスケア企業上位 10 社のうち 9 社、米国の 6 つの軍事機関すべて、その他さまざまな企業が含まれます。Akamai は 1 日あたり 7 億 8,000 万件以上の Web アプリケーション攻撃、260 億件以上のボットリクエストが発生していると見ています。Akamai では、数百人もの脅威リサーチャーやデータサイエンティストが、毎日 932 TB を超える新しいデータを照会して、脅威を検出しています。このような高水準でグローバルな知見と、高度な機械学習、AI、そして人間による分析を組み合わせることで、一般的な攻撃も高度な攻撃も、両方を先取的かつ予測的に阻止することができます。

Akamai は、10 年以上にわたってアプリケーション攻撃を緩和してきました。そして最大規模の攻撃にも耐えながら、お客様を守り、インフラの可用性を維持してきました。新しい脅威の調査、報告を継続しており、攻撃が進化し、規模が拡大して、手口が巧妙化していく中で、Akamai のソリューションは、攻撃の先を行くように革新と改善を続けています。また、App & API Protector は Akamai プラットフォーム上に構築されているため、標準搭載のパフォーマンス機能を通じて、Web サイト、アプリケーション、API のパフォーマンスを最大限まで引き上げることができます。

こちらの無料トライアルをご活用いただき、Web アプリケーション保護と API 保護のニーズを確認し、Akamai App & API Protector のメリットを実感してください。