ホワイトペーパー

WAF から WAAP へ：包括的なアプリおよび API セキュリティソリューションに対する Akamai のアプローチ

目次

はじめに

アタックサーフェスがますます拡大、多様化し、運用上の障壁とコストが増大し、継続的に検知を逃れようとする多次元的な脅威が存在している状況で、セキュリティチームは従来の Web アプリケーションファイアウォール（WAF）を超える可視性を必要としています。具体的には、アプリとアプリケーション・プログラミング・インターフェース（API）のエコシステムの効率を高め、より強力な保護を実現するための自動ツールが必要です。このような保護を表す新しい用語が、Web アプリケーションと API の保護（WAAP）です。ビジネスのセキュリティと顧客の安全を重視する見識のある組織は、デジタル資産全体の複数の脅威に対する包括的な保護を求めています。そのような保護には、既知の攻撃、未知の攻撃、ゼロデイ攻撃からアプリを保護することだけでなく、次のことが含まれます。

- 適応型脅威検知
- ポリシーの自動更新
- 堅牢な DDoS 防御
- API の探索と保護
- ボットの可視化と緩和
- 開発ライフサイクルへの簡単な統合

このホワイトペーパーでは、従来の WAF テクノロジー、WAF から WAAP への移行、WAAP ソリューションの進化を引き起こしている継続的な市場の需要について説明します。セキュリティ分野のリーダーとして定評のある Akamai のアプローチは、エンドユーザーのためにオンラインライフの力となり、守るセキュリティテクノロジーを革新することに重点を置いています。

WAF の従来の定義

従来の WAF は、エンドユーザーと Web アプリケーション間のトラフィックフローの中間に位置します。WAF は、暗号化されていない／暗号化されている HTTP トラフィックが通過する際に、ルールリストで定義されている攻撃がないか検査します。

ほとんどの WAF は事前に定義されたルールリストを使用して、正規の HTTP トラフィックが散りばめられた悪性の HTTP リクエストを識別し、何千もの既知の攻撃から保護します。また、新しい攻撃ベクトルや新たな変更が加えられた既存の攻撃ベクトルが継続的に進化し、脅威アクターによって悪用されています。この場合、従来の WAF のルールを継続的に更新し、正当なトラフィックの特性に合わせて調整する必要があります。正当なトラフィックの特性は、アプリケーションごとに異なり、時間の経過とともに変化します。

より強力な保護と優れたパフォーマンスを求めるエンドユーザーに対応するため、WAF の範囲が拡大し、分散型サービス妨害（DDoS）の緩和、API セキュリティ、ボット緩和機能などの隣接するセキュリティテクノロジーやサービスが含まれるようになりました。このような継続的な進化が起これば、新しい定義や新しい用語が必要になるのは当然のことです。

従来の WAF の課題

WAF を導入した組織は、有効性、管理の容易さ、保護されたアプリケーションや API への影響という点で、WAF が当初の期待に沿っていないと訴えることがよくあります。悪性のコードを見つけるために数十億もの Web リクエストや API リクエストを検査することで Web パフォーマンスの問題が発生することが多いため、WAF は組織内のフリクション、パフォーマンスの低下の原因になったり、セキュリティプロトコルに起因する展開の妨げの原因になったりすることがよくありました。

従来の WAF では、展開に関する重大な課題のいくつかが、次のような要因から発生します。

- 不正確な検知と大量のフォールス・ポジティブ（誤検知）により、アラート疲れや追加のリスクが発生する
- WAF は手作業によるレビュー、調整、メンテナンスに依存している
- きめ細かな制御が欠如しているため、エンドユーザーの体験とビジネスプロセスを妨げる厳格な拒否ポリシーにつながる
- 時代遅れの脅威インテリジェンスにより、脆弱性が増加する
- 制限や柔軟性の欠如により、パフォーマンスとカバレッジが低下する
- デジタル拡張を保護するための制約が多過ぎる

従来の WAF は強力なセキュリティツールです。とはいえ、組織はしばしば、このホワイトペーパーで取り上げる運用上の問題や緩和されていないリスクにさらされ続けています。

WAF テクノロジーを WAAP ソリューションでアップデートしたいと考えている組織は、そのソリューションがビジネス価値と堅牢なセキュリティ保護の両方をもたらすものであることを確認する必要があります。WAF から WAAP へ移行することで、この強力な保護と機能性、効率性、使いやすさが組み合わさり、セキュリティチームと他のチームの両方のビジネスニーズが満たされます。

設計原理：WAF から WAAP へ

従来の WAF 製品はエンドユーザーのルール作成に重点を置いているため、どのベンダーでも WAF ソリューションを構築し、比較的容易に市場に投入できます。これは、オープンソースの Open Worldwide Application Security Project ModSecurity Core Rule Set（OWASP CRS）を中心に構築された商用サービスの普及によって実証されています。

しかし、次のことが可能である包括的な WAAP ソリューションをプロバイダーが設計することは困難です。

- 新しい脆弱性が出現した際にアプリケーションと API を保護するために、インラインで展開する
- 最新のアプリケーション開発手法に対応する
- DDoS 防御、ボット緩和、API 保護、クライアントサイドの Web アプリケーション保護の、同程度に強力なレイヤーを提供する

Akamai は WAAP ソリューションの設計に着手するにあたり、WAAP ソリューションは「及第点」以上のものでなければならないと考えました。App & API Protector は、セキュリティリスクに対処すると同時に、お客様の組織が主要なビジネス目標に集中できるようにするために作成されました。設計の構想として、Akamai は理想的な WAAP ソリューションは次のようなものを提供する必要があると考えました。

効果的なセキュリティ
アプリケーションは、ビジネスのあらゆる側面を動かします。企業のセキュリティチームの基本的な目標は、悪意からアプリケーションを保護することです。セキュリティチームは、トップクラスの検知を実現する WAAP ソリューションを見つけるという課題に直面しています。理想的なセキュリティツールは、WAAP ソリューションの最も重要な側面である検知の有効性を重視しており、ゼロデイ攻撃、悪用、共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）からの防御と可用性に関して確かな実績があります。

正確性
セキュリティチームは、リスクを緩和することとビジネスの迅速な移行を実現することの適切なバランスを見つける必要があります。理想的なソリューションは自己調整メカニズムを備えており、エンドユーザーの体験やビジネスプロセスを犠牲にすることなく誤検知を削減できます。

最新の防御

組織は、新しい脆弱性が発見された際に対処するために、保護を継続的に（多くの場合は手動で）最新のルールに更新する必要があります。これを実現するためには、2 つの重要な機能が必要です。それは、攻撃ベクトル全体にわたる最新のインテリジェンスへのアクセスと、防御戦略を調整して柔軟な攻撃に対処できる熟練したセキュリティリソースです。理想的なソリューションは、脅威インテリジェンスコミュニティのリーダーであり、資産保護の全体でセキュリティ業務をシンプル化する機能を提供します。

適応性

脅威の状況は急速に変化します。AI を利用した攻撃が迫っているなかで、セキュリティチームはこれまで以上にセキュリティ業務の効率を高める必要があります。理想的な WAAP ソリューションは、高度な自動化、機械学習、深いグローバルインテリジェンスを組み合わせて、更新を自動的に配信し、クリック操作で実行できるカスタマイズされたルール変更を提案します。

可視性

従来の WAF ソリューションでは通常、アラートが際限なく続き、セキュリティ担当者による各アラートの慎重な分析に社内リソースが費やされます。より効果的な WAAP ソリューションは、リソースの負荷を軽減するために、攻撃が発生したタイミング、場所、方法を組織に通知することで、マルチソリューションの可視性と攻撃に関するプロアクティブなコンテキストを提供します。

スケーラビリティ

受信トラフィックを処理するための十分なスケーラビリティを備えていないソリューションは、容易に Web レイテンシーを増加させるボトルネックとなり、負荷がかかると崩壊する可能性があります。効果的な WAAP アプローチを取れば、時間によって変化するトラフィックの需要に合わせてシームレスかつ自動的に拡張し、中断やパフォーマンスの低下を招くことなく継続的に保護できます。

連携

効果的なセキュリティソリューションは、現行のスタックに統合でき、プログラム可能で、使いやすく、フリクションレスである必要があります。理想的なソリューションは、セキュリティチームと開発チームの橋渡しをします。

サポート

要求の厳しいセキュリティイベントの発生中、組織はタイムリーな解決策を提供するために必要なスキルとリソースに圧倒されることがよくあります。理想的なソリューションは、定期的なマネージド・サービス・オプションとオンデマンド・サービス・オプションを備えており、アクティブな攻撃、サービスの問題、スタッフの離職、社内スキルセットのギャップなど、よくあるシナリオに対処するための専門知識と緩和を提供できます。

これらの設計原理を念頭に置いて、Akamai がコアテクノロジーを手始めに、主要な WAAP ソリューションである App & API Protector の構築にどのようにアプローチしているかを見ていきましょう。Akamai のソリューションは、多数のセキュリティ製品を 1 つに統合して、アプリケーションのセキュリティ確保、大規模な DDoS 攻撃からの防御、資産全体の API の保護、ボットトラフィックの制御といった課題に総合的に対処します。

WAAP に対する Akamai のアプローチ

ルールセットを超越

市場が従来の WAF 設計原理から最先端の効果的な WAAP のセキュリティソリューションに移行したため、効果的な検知および緩和テクノロジーが依然として注目されていました。

Akamai は、2009 年に独自の WAF を世界初のエッジベース WAF として導入しました。この時点では、セキュリティベンダーは検知の基盤として静的なルールセットをベースとした WAF を提供していました。Akamai は当時、Kona Rule Set と呼ばれる独自のルールベースエンジンを構築することで差別化を図りました。Kona Rule Set は、少数の柔軟なルール（静的ルールではない）と異常（アノーマリ）スコアモデルを組み合わせて、正確性と攻撃の可視性を向上させました。

その後、2017 年に Akamai は自動化された攻撃グループを導入しました。その際、Akamai が管理する保護機能により、組織はルールを継続的に設定および更新する必要がなくなりました。自動化された攻撃グループは革命的であり、すぐに数千ものアクティブな Akamai のお客様の WAF ポリシーでこの新しいアプローチを活用できるようになりました。

Akamai はアプリケーションセキュリティに対するアプローチを継続的に進化させ、統合型のアプリケーションおよび API 保護（ボット防御機能など）に重点を置き、2021 年には App & API Protector の提供を開始しました。これは、企業および拡大するグローバルビジネス向けに Kona Site Defender WAF の代わりに提供することを目指した WAAP ソリューションです。App & API Protector は、Kona Rule Set テクノロジーを Adaptive Security Engine へ最新化することで、セキュリティ業務に対する Akamai のアプローチ方法を一変させました。

レート制限を超えてアプリケーションレイヤー DDoS 防御を最新化

DDoS に関して言えば、レート制限は実績のある効果的なツールです。しかし、高度なレイヤー 7 DDoS 攻撃、マルチベクトル攻撃、API の悪用が増加したことにより、従来の DDoS 防御ではついて行くのが困難になりました。固定しきい値と事前定義されたシグニチャーに依存する静的防御は、事後対応的であり、特に攻撃者が悪性のトラフィックと正当な要求を織り交ぜるようになっているため、誤検知が生じやすいです。そこで、Akamai は DDoS 防御に対するアプローチを変え、URL Protection や Behavioral DDoS Engine などの新たなイノベーションを導入しました。

Behavioral DDoS Engine は、Akamai App & API Protector に最先端の追加機能を提供し、Adaptive Security Engine をコアテクノロジーの 1 つとして加えます。これらのエンジンを組み合わせることで、最新の脅威からのかつてない保護が実現し、Akamai は WAAP のリーダーになりました。このデュアルエンジンアプローチは Akamai の差別化要素であり、自動更新、自己調整機能、コンテキスト認識検知機能によって、人が介在する必要のない体験を実現します。

包括的な保護を実現する単一のソリューション

現在、変化により、アプリケーションセキュリティの再定義が進んでいます。サーバーレス・エッジ・コンピューティング、マイクロサービスベースのアーキテクチャ、シングルページアプリケーション、SaaS ／ IaaS ／ PaaS ／ FaaS アプローチを使用する最新の開発手法により、アプリケーションセキュリティが形作られています。

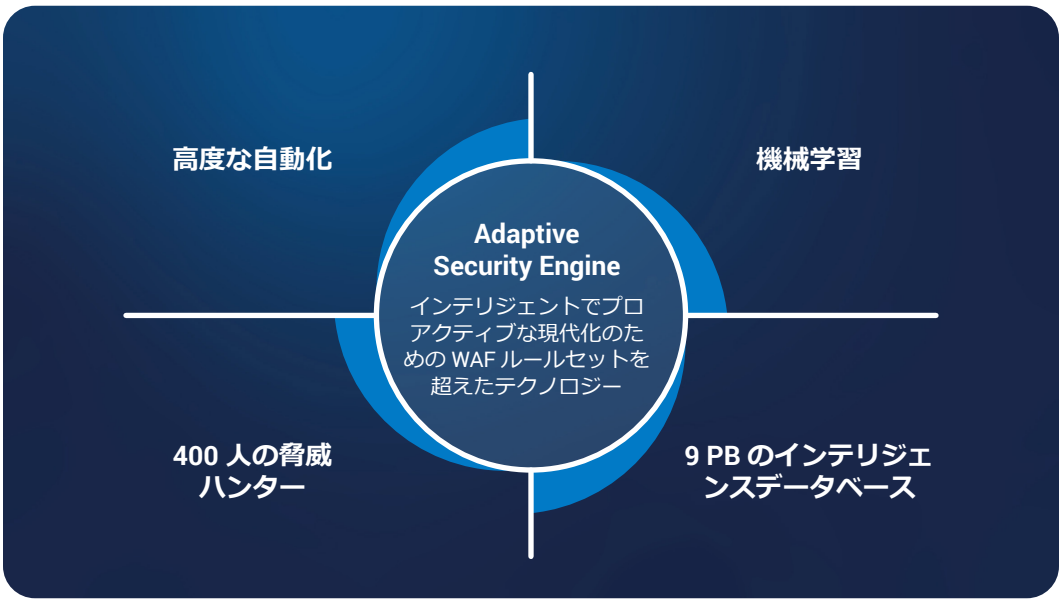
複雑な IT 環境で最新のアプリケーションと API を保護するために、Akamai は、より適応性、柔軟性、包括性の高いアプローチでアプリケーション・セキュリティ・テクノロジーを再設計しました。Akamai の WAAP ソリューションが Web Application Protector と Kona Site Defender から App & API Protector へ移行した際、追加のセキュリティ機能と特徴的なツールセットが組み込まれました。

App & API Protector は現在、数多くの追加のセキュリティ強化機能を提供しており、その機能はすべて、単一のインターフェースで表示および制御できます。Akamai の WAAP ソリューションは、以下の機能を兼ね備えています。

1. Adaptive Security Engine
2. きめ細かな制御が可能なアプリケーションセキュリティ
3. 高度なレイヤー 7 DDoS 防御を含む DDoS 防御
4. 探索および PII 保護機能を含む API 保護
5. ボットの可視化および緩和機能
6. グローバルな拡張性、脅威インテリジェンス、回復力を実現するプラットフォーム

Adaptive Security Engine

Adaptive Security Engine は、機械学習（ML）、リアルタイムのセキュリティインテリジェンス、サイバーセキュリティのエキスパート、高度な自動化を組み合わせて、次世代の保護を提供します。Akamai の検知と防御のコアテクノロジーである Adaptive Security Engine は、人が介在する必要のないアプローチで Web アプリケーションと API 資産全体を保護できるようにします。また、WAF から WAAP への Akamai の進化を促進し、ボットマネージャー、DDoS 防御、DevOps 統合など、相互に関連するセキュリティソリューションを取り入れています。



Adaptive Security Engine は、顧客ごとに固有のトラフィックと攻撃のパターンを学習し、すべてのリクエストの特性をリアルタイムで分析して、その知識を将来の脅威に対する迎撃や適応に利用するという点で、独自性があります。同じプラットフォームの知見とインテリジェンスを使用し、調整を提案することによって誤検知を減らします。この自己調整機能は、適応型脅威防御をプロアクティブな更新として提供するため、セキュリティチームや開発チームにとって使い勝手が良いものとなっています。

適応型脅威検知

このエンジンは、プラットフォームのインテリジェンスと各リクエストのデータ／メタデータを組み合わせる多次元的な脅威スコアリングモデルを採用しています。このデータは、真の攻撃を正確に特定するための意思決定ロジックで処理されます。

巧妙な攻撃者は、独自のアプローチにより多くの時間と労力を費やします。そのため、適応型検知は、防御をすり抜ける標的型かつステルス型の攻撃を特定する上で特に効果的です。攻撃者が脆弱性や設定ミスを調べると、Adaptive Security Engine はその戦術に関する証拠を収集して相互に関連付け、攻撃者のこれまでの特徴をより識別しやすくします。

実際のペイロードと対象リクエスト内の位置の他に、Adaptive Security Engine がクライアントごとに評価する攻撃ディメンションの例として、以下のようなものがあります。

- 偵察や攻撃の履歴（頻度、規模、重大度など）
- 悪性の自動化ツールや攻撃ツールの兆候
- 攻撃トラフィックの既知の発生源との相関性

さらに、Adaptive Security Engine は 2 つの独自のテクノロジーによって強化されています。それは、入力内容をトークン化してフィンガープリントに変換し、精度の高い検知を行う「Smart Detect」と、リクエストボディの正しいコンテンツタイプを検知し、コンテンツの操作やバイパスを防止する「Smart Sniff」です。Akamai の脅威研究者は、Akamai の広範なインフラとシステムを活用して、すべての本番環境のトラフィックで新しい検知をパッシブに実行し、ML モデルを使用してその結果を分析します。

自動更新

今日の多くの組織には、発展中の脅威を継続的に追跡し、構成を更新し、Web トラフィックに対して再テストを行ってポリシーを最適化するための十分なリソースやセキュリティの専門知識がありません。これに対して、Akamai は AI ／ ML 自動テストフレームワークを使用して Adaptive Security Engine を継続的に更新し、変化する脅威に対応しながら高い精度を維持します。この更新により、公表前のゼロデイ攻撃から保護されることが多々ありました。

正確性を確保するためのテストフレームワーク

WAAP ソリューションのテストは、シンプルな前提に基づいています。それは、さまざまな攻撃ベクトルをテストし、Web 攻撃を阻止することです。ただし、次の要因を考慮する必要があります。

- 実際の環境はテスト環境よりも複雑なため、誤検知やフォールス・ネガティブ（検知漏れ）につながることがよくあります。
- 正確性を考慮してテストフレームワークを設計するためには、さらなる検証が必要になります。攻撃を検知できたかどうかだけではなく、誤検知や検知漏れを誤ってトリガーすることなく検知できたかどうかを検証する必要があります。
- テストには、本物の Web トラフィック（正当なトラフィックと攻撃トラフィックの両方）を使用する必要があります。

Adaptive Security Engine のアップデートは、正当なトラフィックに悪影響を与えないように、複数の段階で構成されています。

- 誤検知を生じさせることなく、攻撃を適切に捕捉できるようにするために、すべての検知が合成トラフィックを使用してラボでテストされます。
- 続いて、実際の本番環境のトラフィックで更新がテストされ、サンプルが現在のプラットフォームトラフィックに対して有効であることが確認されます。このプロセスでは、実際の顧客のトラフィックに対してシャドウモードで更新を実行します。シャドウモードで実行すると、顧客のトラフィックに影響を与えずに検知の正確性をテストすることができます。
- 更新が第 2 段階を通過すると、人間の分析で見落とされた可能性のあるパターンやトリガーを ML が特定し、その後脅威リサーチチームが手作業で結果をレビューします。
- このような各段階のチェックに合格した場合のみ、変更が次のフェーズに進み、ネットワークのより大きなセグメントに展開されます。100% 展開された後、自己調整機能により、顧客のトラフィックパターンに固有の誤検知が解消されます。

自動的な自己調整

手動調整の場合、ポリシーが古くなったり、人的ミスが発生したりする可能性があります。しかし、自動的な自己調整であれば、手動調整の負担が軽減され、人がほぼ介在する必要のない体験が実現します。Adaptive Security Engine は、各セキュリティポリシーのすべてのトリガーに ML、統計モデル、ヒューリスティックを適用して、実際の攻撃と、攻撃として誤認されたエンドユーザートラフィックを正確に区別します。これは、オンボーディング中にのみ適用される一般的なプラットフォーム全体のチェックではなく、エンドユーザーの設定や介入なしで 24 時間継続的に実行される調整プロセスです。

自己調整はフリクションレスで、シンプルです。セキュリティ管理者は、ユーザーインターフェースをワンクリックするだけで簡単に推奨事項を確認して受け入れることができます。また、AppSec API、コマンドラインインターフェース（CLI）、または Terraform を使用して自動化することもできます。透明性を高めるため、事前にフィルタリングされた Web Security Analytics へのリンクには、誤検知と判断されたすべてのリクエストが表示され、各調整推奨事項に対する根拠が示されます。

設定と自動化の柔軟性

WAAP ソリューションベンダーが従来のルールセットテクノロジーから脱却すると、設定と自動化の柔軟性が向上します。Adaptive Security Engine は、次の機能を提供します。

- アプリケーションやそれに関連するリスク選好に応じて、さまざまな種類の WAF 更新（自動または手動）を用意する
- アプリケーション／トラフィックのふるまいが標準的でない場合、攻撃グループごとのアクションと、カスタマイズに必要な関連ルールを制御する
- IP、ジオ、ヘッダー、ペイロードなど、さまざまなリクエスト特性に対応するシンプルな条件や複雑な条件を設定する
- アプリに対して疑わしい WAF 攻撃やスキャンを実行していることが検知された脅威ソースを、ペナルティボックスによってプロアクティブに緩和する
- デバッグヘッダーを修正する
- リクエストペイロード検査サイズまたは攻撃ペイロードロギング設定を変更する
- 検知ロジックの変更のシミュレーションを実行し、自信を持ってその変更を本番環境に適用できるようにする

実世界での検証

評価モードでは、Akamai のお客様が特定の Adaptive Security Engine バージョンを柔軟かつきめ細かく設定し、アップデートや新しいルール／ポリシーをテストすることができます。お客様は、新しい更新や変更を有効化する前に、特定の Web アプリケーション環境に適切であるか、または必要であるかを確認できます。効果的にセキュリティを最新化する上で、Akamai は、過去のトラフィックでテストするよりも、リアルタイムのトラフィックでテストする方がセキュリティが向上すると考えています。評価モードは、ポリシーが適用されているかのようにリアルタイムの結果を確認できるシャドウルールを適用するのと似ていますが、現在のエンドユーザーには影響しません。組織は、この手動／評価モードを選択することで、誤検知や検知漏れへの予期しない影響を最小限に抑えることができます。

近代的な保護の統合

セキュリティチームと DevOps チームは、CLI、Akamai Terraform、または CI/CD 自動化パイプラインのスクリプトを使用して Akamai API へのコールを統合することで、セキュリティを管理することもできます。柔軟な設定と自動化が可能なため、強力なセキュリティ機能によって開発速度が妨げられることはありません。これらの統合では、次のことを行えます。

- アプリケーションの迅速なオンボーディングを実現する
- 大規模なアプリケーションポートフォリオ全体でセキュリティポリシーを統一的に管理する
- ハイブリッドインフラやマルチクラウドインフラ全体でセキュリティの適用を一元化する
- GitOps ワークフローで DevOps チームとセキュリティチームのコラボレーションを改善し、最適なカバレッジを実現する

また、セキュリティ情報およびイベント管理（SIEM）により、Akamai プラットフォームで発生するセキュリティイベントを収集できます。そして、Akamai の SIEM 統合ソリューションは、SIEM イベントデータをオンプレミスおよびクラウドベースの SIEM 分析ツール（Splunk や QRadar など）に配信する方法を提供します。これにより、4 つの基本的なステップで Akamai セキュリティイベントを自社の包括的なイベント管理およびセキュリティインフラに組み込むことができます。

次の機能や設定により、データフィードを保護および制御できます。

- **イベントフィルタリング**
  セキュリティ設定とセキュリティポリシーを使用することで、実際の脅威に集中できるようになります。
- **データ保持**
  コレクターは 12 時間分のデータを保存するため、見落としたイベントを捕捉できます。
- **SIEM 過負荷防止**
  SIEM コネクターでは、各リクエストで取得されるセキュリティイベントの最大数を設定できます。これにより、SIEM アプリケーションが過負荷状態になるのを避けることができます。
- **取得頻度**
  SIEM コネクターが SIEM API を呼び出してセキュリティ・イベント・データを取得する頻度を設定できます。

アプリケーションセキュリティと DDoS 防御

アプリケーションセキュリティは現代のサイバーセキュリティの重要な要素であり、さまざまな脅威や脆弱性に対するアプリケーションの回復力を常に確保します。アプリケーションセキュリティは、いくつかの重要な領域において重視されます。特に重要なのは、データの完全性と機密性においてです。なぜなら、アプリケーションセキュリティによって機微な情報が不正なアクセスや改ざんから保護されるからです。また、アプリケーションセキュリティは、セキュリティインシデントに起因する混乱からアプリケーションを保護し、一貫したサービス可用性を確保することにより、事業継続性においても重要な役割を果たします。さらに、アプリケーションセキュリティはレピュテーション管理に不可欠であり、組織の評判や顧客の信頼を損なう可能性のある侵害を防止します。最後に、アプリケーションセキュリティは、組織が規制要件を遵守し、法的罰則や罰金を回避するのに役立ちます。

機能面では、WAAP ソリューションは Web アプリケーションとインターネットの間の HTTP トラフィックのフィルタリングと監視を行います。これにより、XSS、SQL インジェクション、DDoS などの一般的な Web ベースの攻撃から保護されます。

App & API Protector は、リソースを過負荷状態にすることを目的とした大規模攻撃に対抗するように設計された、市場トップクラスの DDoS 防御機能を備えていることが評価されています。このソリューションは、次の方法で DDoS に対抗します。

- **エッジベースの DDoS 緩和機能**
  App & API Protector は、Akamai のグローバル分散型エッジプラットフォームを活用することで、DDoS 攻撃がアプリケーションオリジンに到達する前に即座に阻止できます。このエッジファーストのアプローチは、アプリケーションのパフォーマンスに影響を与えることなく、最小限のレイテンシーと最大限の保護を実現します。

- **レート制限**
  App & API Protector には、分散されたアプリケーションレイヤー DDoS 攻撃を防ぐための適応型レート制限が含まれています。この制御は、IP、ジオ、IP レピュテーション制御、さまざまな HTTP ヘッダー、一致条件などの多様な基準に基づいて受信リクエストのレートを制限するように設定できます。

- **インテリジェントな負荷制限による URL 防御**
  制限による URL 保護では、レート制限のアプローチが異なります。URL 保護により、オリジンのキャパシティに応じて許容されるリクエストレート（最大 RPS）に基づいて、オリジンを過剰なリクエストから保護できます。高度に分散されたアプリケーションレイヤーの DDoS 攻撃から、コンピューティング負荷の大きい URL や API エンドポイントなどを保護するように特別に設計されています。

- **Behavioral DDoS Engine**
  App & API Protector の新機能である Behavioral DDoS Engine は、多層防御戦略のための強力なツールです。トラフィックのベースラインの確立と標準に反する異常の特定に ML を使用することで、人が介在する必要のないアプローチによる DDoS イベントの管理と緩和を導入します。このエンジンは、変化するトラフィックパターンを把握することで機能します。ユーザーは明確なしきい値を設定することなく、さまざまな異常にシステムがどのように反応するかを定義できるため、システムの管理と調整を行わなければならないという運用上の負担が軽減されます。

- **自動更新と適応型の自己調整**
  Akamai の戦略的な 2 つのエンジン（Adaptive Security Engine と Behavioral DDoS Engine）を使用する App & API Protector は、自動更新と ML を活用した自己調整により、新たな脅威に継続的に適応し、運用上の負担を軽減します。

Behavioral DDoS Engine の仕組み

Behavioral DDoS Engine の中心は、リアルタイムのトラフィックを継続的に監視し、正常なふるまいのベースラインを確立し、攻撃を示す逸脱を即座に検知する高度な ML モデルです。発信元の国、TLS パターン、IP、TLS フィンガープリントなど、複数の動的な要素に関してトラフィックパターンを分析することで、このエンジンは異常を迅速に特定し、対策を講じることができます。

Behavioral DDoS Engine の主なコンポーネントは次のとおりです。

- **リアルタイムのふるまい監視**
  このエンジンは、トラフィックを継続的に分析して、通常のアクティビティのベースラインを確立し、DDoS 攻撃の可能性を示唆する逸脱を即座に検知します。

- **機械学習による正確性の確保**
  このエンジンは、高度な ML モデルを使用してトラフィックパターンのかすかな異常を特定し、正当なユーザーをブロックすることなく正確に緩和することができます。

- **予防型の緩和**
  このエンジンは、Akamai のグローバルネットワークの知見（1 日あたり 1,056 TB のトラフィック）を活用し、攻撃を予測して無効化します。多くの場合、攻撃がビジネスに影響を及ぼす前に実行されます。

- **多次元的な分析**
  IP、国、TLS パターンなどの複数の要素に関してトラフィックを評価し、各アプリケーションのニーズに合わせて堅牢な保護を提供します。

高度なアーキテクチャによる超高性能な防御
Behavioral DDoS Engine は、複数の重要な要素を統合した高度なアーキテクチャを基盤としています。

- **検出エンジン**
  動的な要素と過去の攻撃データを使用して、DDoS 攻撃をリアルタイムで特定します。
- **緩和エンジン**
  ベースラインジェネレーターからのインテリジェンスと脅威信号を使用して攻撃に自動的に対処し、セキュリティチームの運用オーバーヘッドを削減します。
- **ノイズ／誤検知削減**
  ML モデルが無関係のデータを除去し、クリーンなトラフィックが分析や緩和に使用されるようにします。
- **ベースライン生成機能**
  クリーニングされたデータを 2 週間にわたって処理することで、トラフィックプロファイルを継続的に改良し、エンジンが常に最新の攻撃戦略に更新されるようにします。
- **ベースライン評価機能**
  AI によって支えられているこの重要なコンポーネントは、毎月数百件もの DDoS 攻撃を評価し、ソリューションを微調整します。

この自動化されたフレームワークにより、セキュリティチームは Behavioral DDoS Engine を使用して、手動操作なしで動的に防御を調整できます。このソリューションは、ボットで生成されたトラフィックや DDoS 攻撃などの異常なトラフィックアクティビティを検知して除去し、アプリケーションを効果的に保護します。

アプリケーションセキュリティの正確性

アプリケーション・セキュリティ・ソリューション（WAF または WAAP）が正確でない場合、日々のアラート件数が増加し、それを管理するためにより多くの内部リソースが必要になります。正確性が低いと、誤検知（悪性ではないリクエストが悪性としてフラグ付けされる）や検知漏れ（悪性のリクエストが悪性ではないとフラグ付けされる）が多数発生し、これらのタイプのアラートの調査と分析に貴重なセキュリティ・スキル・セットと時間が浪費されてしまいます。

多くの場合、制御の範囲が広すぎることや、修正機能が過剰であったり不足していたりすることが原因で、組織はアラート疲れという課題をしばしば抱えていますが、解決策がない状態が続いています。そのため、組織は WAF をオフラインにしたり、さらにひどい場合はアラートやバージョンの更新を無視したりすることがよくあります。これにより、多くの組織にとって、正規ユーザーを誤ってブロックする懸念は軽減されますが、Web 攻撃や API 攻撃に対する保護は十分ではなくなります。また、多くの組織では制御のきめ細かさが欠けているため、正当なトラフィックに対するアクセス許可と悪性トラフィックの正確なブロックのバランスを取ることができません。

効果的な WAAP ソリューションの利点は、誤検知と検知漏れの両方を低減して正確性を向上させ、包括的な WAAP 制御および機能によって正規ユーザーへの影響を最小限に抑えることです。

正確性を理解する

正確性とは、正規ユーザーを誤ってブロックせずに攻撃を阻止する WAF や WAAP の能力の尺度であり、次の 4 つの変数が考慮されます。

- **正検知（TP）：**悪性であると適切に識別された実際の攻撃
- **誤検知（FP）：**悪性であると誤って識別された正当なリクエスト
- **負検知（TN）：**許可されてアプリケーションに渡された正当なリクエスト
- **検知漏れ（FN）：**不適切にアプリケーションに渡された実際の攻撃

Client Reputation スコア

Client Reputation は、高度なリスク分析エンジンを使用して、サイトへのアクセスを試みる各 IP アドレスの一連の「リスクスコア」を計算します。受信 IP アドレスを分析し、攻撃者の固執度、標的となるアプリケーションの数、攻撃の深刻度、規模、業界、顧客のアプリケーションを標的とした過去の攻撃などのさまざまな要素を使用して、この IP アドレスが次のような Web 攻撃に関与するものである可能性を示すスコアを決定します。

- **DOSATCK**
  ボットネットを使用してサービス妨害（DoS）攻撃を開始します。DoS 攻撃の目的は、大量の偽のリクエストをサイトに送りつけて、サイトを耐えられないほど低速にしたり、クラッシュさせたりすることです。分散型サービス妨害（DDoS）攻撃では、このようなリクエストが何千もの場所（通常はマルウェアに感染したコンピューターや電話）から送信されるため、特定の IP アドレスをブロックするだけでは攻撃を阻止できません。

- **SCANTL**
  スキャンツールを使用すると、SQL インジェクション、クロスサイト・リクエスト・フォージェリー（CSRF）、無効なリダイレクト、その他の脆弱性などの潜在的なセキュリティリスクを特定できます。自社のサイトに対して Web スキャンツールを実行するのは良いことですが、Web サイトに対して悪意のある人物がスキャンツールを実行するのはあまり良いことではありません。

- **WEBATCK**
  SQL インジェクション、リモート・ファイル・インクルージョン、クロスサイトスクリプティングなどの手法を使用して、マルウェアのインストールやユーザーデータの窃取などを行います。ハッカーは、パスワード、クレジットカード番号、社会保障番号、ユーザーデータベースに保存されているその他の情報など、あらゆるユーザーデータを取得できる可能性があります。

- **WEBSCRP**
  自動化されたツールを使用して Web ページのコピーをダウンロードし、そのページのすべてのコンテンツを「スクレイプ」（つまり、コピー）します。そのコンテンツは、違法または非倫理的な用途に転用される可能性があります。

Client Reputation を使用すると、蓄積された脅威インテリジェンスを Akamai Connected Cloud から取得し、それに基づいて疑わしい脅威ソースから組織をプロアクティブに保護できます。

マルウェア防御

脅威アクターはマルウェアを一般的な攻撃戦術として使用します。アプリケーションを包括的に保護するために、Akamai はマルウェアから防御するソリューションを提供しています。あらゆる規模の組織が、効率を高めるために社内外からのファイルのアップロードを許可しています。その一般的な用途は次のとおりです。

- 求人応募用の履歴書
- 雇用契約、オンボーディング、E-Verify、口座振込の設定など
- ローン、アカウント設定、クレジットリクエストなどの申請
- 自動車や住宅などの保険や修理の見積り
- 保険や患者アカウントの設定のための医療記録
- 画像を含む顧客の製品レビューや体験レビュー

アプリ内のマルウェア防御や API セキュリティは、マルウェアの脅威を検知し、標的の企業システムに到達する前にエッジで隔離します。組織は、アプリケーションと API をマルウェアから守り、時間、予算、生産性、社内データ、顧客データを保護できます。

- **エッジでマルウェアを検出して阻止**
  スキャン時にマルウェアが既に拡散している可能性のあるサーバーでのスキャンされるリスクを回避できます。
- **複雑さを回避し、アップタイムから解放**
  ICAP およびエージェントベースのスキャナーのように、システムごとに保護を設定するのではなく、ファイルを一度にスキャンできます。
- **成長に合わせたセキュリティポスチャの設定**
  予防的かつ多層的なアプローチを選択することになるため、組織はビジネスの成長に合わせて保護をスケーリングし、エッジで保護を強化したり、オリジンで再度スキャンしたりすることができます。
- **アプリケーションの一貫性を実現**
  アプリケーションの一貫性を確保するために、アプリケーションコードを設定したり変更したりする必要はありません。マルウェア防御は、Akamai Connected Cloud で完全にホストされます。

アプリケーションセキュリティ分析

App & API Protector には、最も愛されている（最も使用されている）Akamai の製品が含まれています。それは、Web Security Analytics です。この Akamai WAAP ソリューションを使用すると、Akamai プラットフォーム上の Web ブアプリケーションや API に対して発生するセキュリティイベントを捕捉し、提供されるセキュリティ分析ツールでそれを視覚化できます。

Web Security Analytics は、現代のサイバーセキュリティの重要な要素であり、Web トラフィックと潜在的な脅威に関する包括的な知見を提供します。トラフィックパターン、ユーザーのふるまい、セキュリティイベントなどのさまざまなデータポイントを分析することで、Web アプリケーションのセキュリティポスチャを詳細に可視化できます。このプロアクティブなアプローチにより、組織はより効果的に脅威を検知して対応できるようになり、重大な損害が生じる前にリスクを緩和できます。Web Security Analytics は、ボット攻撃、SQL インジェクション、クロスサイトスクリプティングなどの悪性アクティビティを特定するだけでなく、Web アプリケーション内の脆弱性を把握して対処するのに役立ちます。さらに、セキュリティポリシーと規制要件を遵守していることを示すレポートを生成することで、コンプライアンスをサポートします。

API Discovery および Profiling 機能

組織は API を使用し、多くの場合、バックエンドのデータやロジックを公開して新しい革新的な製品を開発することで、強力な Web 体験やモバイル体験を生み出すことができます。その一方、API によりアタックサーフェスが拡大します。組織は、環境内にある API エンドポイント、API の関数、トラフィックプロファイルを把握する必要があります。Akamai の API Discovery および Profiling 機能は、それだけでなく、自動的かつ継続的に実行されます。

API Discovery 機能は、セキュリティチームに対して、組織内のさまざまな業務に関連する未保護の新たなアプリや API のアラートを発行します。この自動検知テクノロジーは、Akamai の WAAP ソリューションの新機能であり、開発チーム、事業部門リーダー、セキュリティチームが常に連携できるようにします。

Adaptive Security Engine は、レスポンスのコンテンツタイプ、パス特性、トラフィックパターンに基づくスコアリングメカニズムを通じて、24 時間ごとに API を自動的に探索します。探索データには、観測された API 仕様に関する情報と以下の詳細が含まれます。

- ホスト名
- ベースパス
- リソースパス
- パラメーターとそのデータ型
- メソッド
- API のフォーマット

ベースパスとリソースパスは、API トラフィックを伴う特定のホスト名で観測されたトラフィックからパスの深さ、子の数、およびシブリングを考慮するアルゴリズムに基づいて決定されます。リソースパス内で、特定のメソッドであることを示すパラメーターが観測された場合、そのパラメーターがマークされ、そのパラメーターのデータ型が特定されます。

API エンドポイントのトラフィックプロファイルには、API の目的と現在の脅威レベルに関する知見を提供する情報が含まれています。具体的には、以下のデータポイントが含まれます。

- API が最初に検出されてから送信されたリクエストの合計（過去 24 時間および長期の傾向）
- API が最初に検出され、最後に確認された日付
- GET、PUT、POST、DELETE、OPTIONS などの異なるメソッドでのリクエストの件数
- 2xx、3xx、4xx、5xx レスポンスを生成するリクエストの数
- ユーザーエージェントに基づくエンドクライアント識別
- クライアントサイドおよびサーバーサイドのエラーにより生じたトラフィックの割合などの応答エラー
- 既知の脅威アクターによるヒット回数（既知の攻撃者から Akamai プラットフォームに送信されたトラフィックの割合を含む）を、Web 攻撃者、Web スキャナー、スクレイパー、DoS 攻撃者に分けて表示

API の保護は、可視性がなければ、大きな障害になる可能性があります。組織は、見えないものは防御できません。Akamai を使用すると、企業は、エンドポイント、定義、リソース、トラフィック特性などの API を自動的かつ継続的に検出し、プロファイリングできます。API が特定されると、Akamai が、DoS、悪性のインジェクション、Credential Abuse 攻撃、API 仕様の不正利用に対処するための広範な保護を提供します。クラウドおよびオリジンに依存しない Akamai のアプローチにより、エンドユーザーが追加の設定を行うことなく、アプリケーション全体で API を簡単に検出できます。こうした可視性が提供されることで、開発者、アプリケーション所有者、セキュリティチームは、新しく、未知の変化する API に対処しやすくなり、そのような API を簡単に登録して防御することができるのです。

ボットの可視化と緩和

ボットは Web サイトトラフィックの半分以上を占めているため、どのボットが組織の目標達成に役立っているか、どのボットが害を及ぼすことを目的としているかを把握するのは困難です。良性ボットは、評価、会話、提案を自動化することにより、組織の効率を高めます。悪性ボットはトラフィックパスを詰まらせ、顧客体験や業務体験に影響を与え、収益を変動させる可能性があります。App & API Protector は、ボットの可視化と緩和によって強力な検知を実現し、悪性ボットをブロックしながら、良性ボットを確認して通過させます。これにより、組織は次のことを行えます。

- **ボットを確認してその影響度を把握**
  検索、サイトパフォーマンスのチェック、ビジネスパートナーとのやり取りなどの操作にボットが広く使用されていることを考えると、現代のデジタルビジネスではボットトラフィックの可視化が極めて重要です。
- **運用上の管理性を向上**
  悪性ボットをブロックすることで、効率性を高め、ビジネスリスクと財務リスクを軽減し、IT 支出の管理を改善することができます。
- **データに基づく的確な意思決定**
  詳細な分析とレポートは、カスタマージャーニー、セキュリティポスチャ、リスク許容度、IT 運用に関して、創造的かつ効果的な選択を行うために役立ちます。

App & API Protector に備わっているボット可視化および緩和機能

App & API Protector は、Web プロパティのパフォーマンスとセキュリティに悪影響を及ぼす可能性のあるボットトラフィックの検知と制御を行います。時間が経つにつれて発展するボット関連の異常や脅威をプロアクティブに監視するために、早い段階で可視化します。

App & API Protector で提供される Akamai のボットソリューションを使用することで、次のことを行えます。

- Akamai にとって既知である 1,700 以上の定義済みボットへのアクセス
- リアルタイムのボットトラフィックの可視化
- カスタムボット定義の作成
- 良性ボットの許可と悪性ボットの拒否
- ボットの可視性とトレンドに関するレポートの確認

高度なボット問題を抱えているサイト向けに、Akamai は Bot Manager を提供しています。Bot Manager には、E コマースとデジタルセキュリティを強化する高度なボット防御機能が備わっています。Bot Manager では、次のような攻撃に使用される持続的な悪性ボットに対して、より繊細なアクションが提供されます。

- Credential Stuffing
- 在庫の買い占め
- コンテンツスクレイピングと価格スクレイピング
- ビジネスロジックの悪用

主なボット機能

Akamai は、WAAP によるボット管理に対するニーズが高まっていることを認識しており、ボット可視化および緩和ツールを強化して、次のような機能を新たに組み込んでいます。

- **ブラウザー内のなりすまし検知機能**
  顧客から好評を得ているこの Akamai Bot Manager の機能は、動的スコアリングモデルと ML を使用してブラウザー内のボットアクティビティを識別して対処します。この機能は App & API Protector に含まれています。
- **条件付き応答アクション**
  顧客はブラウザー内のボットアクティビティについて理解を深め、条件付き応答アクションによって対応し、悪性ボットに対してさまざまな対応戦略を適用できるようになりました。
- **チャレンジアクション**
  さまざまなチャレンジアクションによってボットに対処します。解けない場合にコンテンツへのアクセスをブロックできるようにするインタースティシャルチャレンジなどがあります。

WAF を上回る Akamai ソリューションのメリット

WAAP に対する Akamai のアプローチの結果として、App & API Protector が生まれました。しかし、WAAP のお客様にメリットをもたらす製品は 1 つだけではありません。Akamai Connected Cloud は、最も分散されたグローバルプラットフォーム上に構築され、何百人もの脅威専門家によって支えられており、パフォーマンス、可用性、インテリジェンス、専門知識、効果的なセキュリティをもたらします。

脅威インテリジェンスと検知

強力な社内の脅威インテリジェンス機能を導入すれば、進化する脅威への WAAP ベンダーの対応能力が向上します。一方で、提供されたインテリジェンスの品質、時宜性、実行可能性によって、アプリケーションセキュリティの効果への影響度が決定されます。Akamai は、Akamai Connected Cloud を通じて利用可能なデータを継続的に分析し、脅威環境の現在の傾向や、Akamai が最初に見つけた新たな攻撃ベクトル、さらには現在活動中の攻撃者を識別します。その後、Akamai はそのインテリジェンスを独自の WAAP ソリューションに複数の方法で組み込みます。

このホワイトペーパーで前述した Akamai Adaptive Security Engine は、2 階層の深い脅威インテリジェンスを組み合わせて、強力な独自のエンジンを構築し、お客様の代わりに最新の保護を自動で管理します。Adaptive Security Engine は、ML や自動ルール導入に加え、Akamai のグローバルプラットフォームや大規模な脅威研究者チームから得られる脅威インテリジェンスを備えています。

Akamai プラットフォームインテリジェンス

Akamai には最大規模のグローバルプラットフォームがあるため、すべての Akamai のお客様が世界規模でタイムリーに攻撃トラフィックを分析するメカニズムを利用できます。Akamai のインテリジェンスデータベースには、1 日あたり平均 1,056 TB の攻撃データが含まれています。トラフィックが膨大で頻繁に攻撃されている数千ものオンライン企業の Web トラフィックについて、Akamai の可視化機能を活用し、Akamai の脅威リサーチチームによる分析のために次のような関連する高品質のデータを取得します。

- **WAAP トリガー**
  Akamai の世界中の WAAP から直接データを取り込み、すべての Akamai セキュリティのお客様を標的とした実際の攻撃イベントを捕捉します。
- **CDN ログ**
  Akamai のすべてのお客様から取得したイベントログに対して実行されたオフライン分析を取り込みます。これには、WAAP ソリューションを展開していないお客様も含まれます。

Akamai のインテリジェンスデータベースには、世界最大規模のデータセット（9 PB）が格納されています。事業や顧客のセキュリティを重視する組織にとって、Akamai の脅威インテリジェンスは WAAP ソリューションプロバイダーの最先端を行っています。

脅威リサーチとインシデント対応

脅威リサーチとインシデント対応を担当する組織は、ヒューマンインテリジェンスと分析を活用することで、WAAP ソリューションの攻撃対応範囲を補完し、拡大しています。Akamai では、さまざまな特権を持つ複数のチームにより WAAP のお客様をサポートするとともに、追加の保護が必要となる可能性のある新しい攻撃ベクトルを識別しています。

脅威リサーチ

Akamai 脅威リサーチチームは、Akamai の顧客ベース全体にわたってウェブ攻撃の傾向を定期的に分析しており、さらには必要に応じて個々のお客様のカスタム分析を行っています。また、このチームは、主要な WAF ルールロジックや Client Reputation の作成と更新をサポートするために、実用的なインテリジェンスをクエリーするヒューリスティックを設計および実装を行います。

インシデント対応

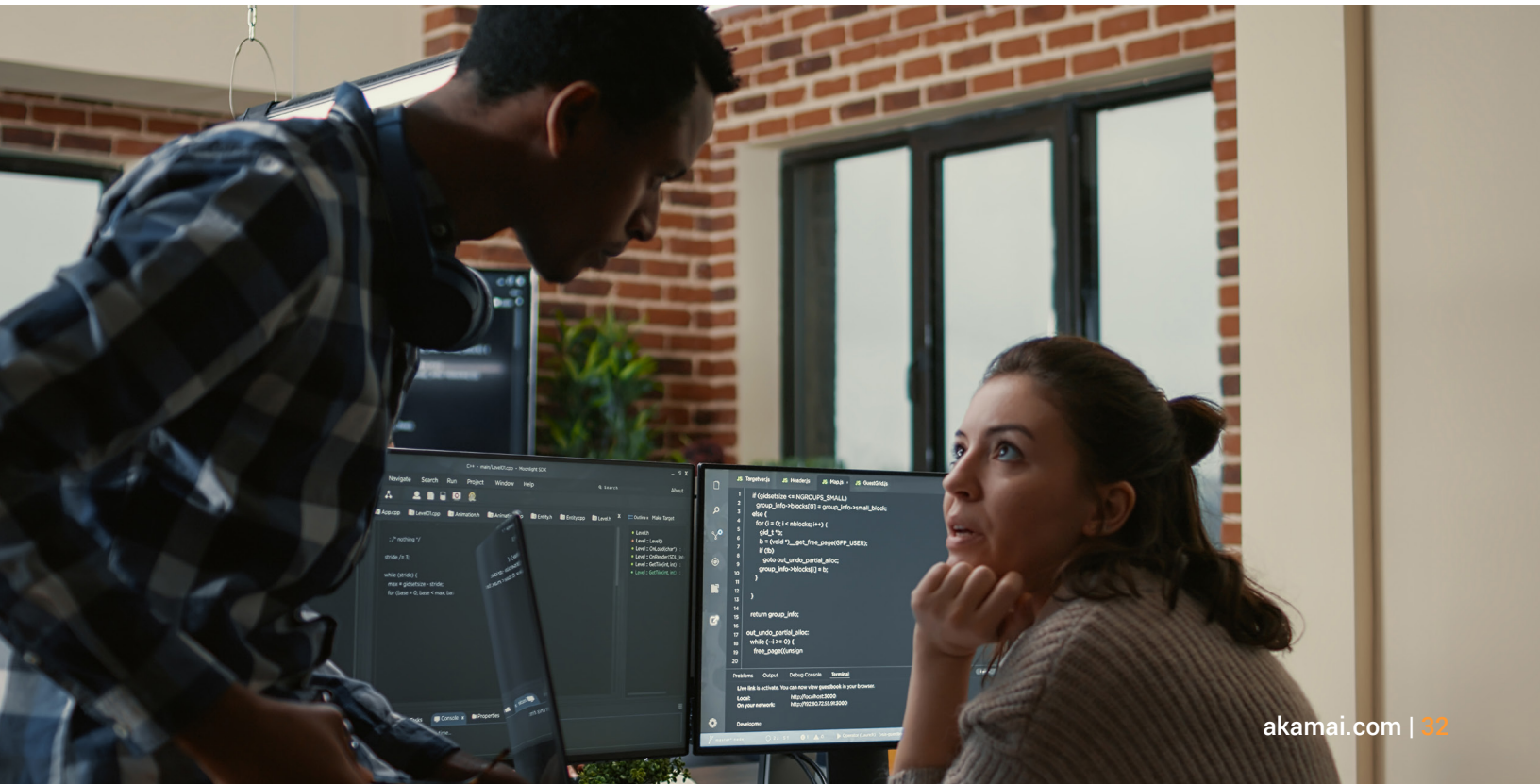
Akamai は、Computer Security Incident Response Team（CSIRT）と Security Emergency Response Team（SIRT）の 2 つのインシデント対応チームを運営しており、これらのチームが Akamai のグローバル・セキュリティ・オペレーション・センター（SOC）と協力して、個々のお客様が攻撃を受けた際の分析とインシデントへの対応を行っています。さらに CSIRT は、さまざまな業界を代表する、頻繁な攻撃を受けている Akamai のお客様を、新たな攻撃ベクトルや傾向の主な指標として監視しています。

迅速な脅威検知

新しい機能により、新たな脅威や注目度の高い CVE に対する保護を迅速に展開できます。自動更新と「Akamai が管理する」アクションのオプションにより、防御を機敏に管理できます。

CVE 保護

Akamai 脅威リサーチチームは、共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）を継続的に監視し、WAAP ソリューションが更新されて顧客のアプリケーションを保護し、Akamai CVE ルックアップツールを通じて必要な確認を提供します。このツールは、脅威レベルや Akamai の現時点での保護に関する知見など、CVE に関する詳細な情報をもたらすため、役に立ちます。Akamai の CVE 保護カタログは、Akamai の保護に合わせてセキュリティ対策を優先するための可視性を提供します。顧客は CVE データベースを検索して、脆弱性に対する Akamai のアクティブな保護対策を判断するとともに、脅威レベルの評価や CVE の詳細へのアクセスを行えます。



グローバル分散型エッジプラットフォーム

信頼性と回復力

上質な WAAP ソリューションは、大規模なサイバー攻撃が発生しても顧客のトラフィックを制限しない、広範で強力なネットワーク上に構築されています。WAAP プロバイダーのグローバルプラットフォームが定評のある品質、キャパシティ、実行能力を備えていることは、ソリューションの機能と同じくらいに重要です。WAAP プロバイダーがアクティブな攻撃中に良性のトラフィックを配信できない場合、顧客はソリューションに投資したのかツールに投資したのかを評価する必要があります。

Akamai は、業界をリードするパフォーマンスと保護をお客様に提供することに注力しています。このミッションは、極めて強固な基盤上にサービスを構築することによってのみ達成できます。その強固な基盤とは、Akamai Connected Cloud です。Akamai は、130 か国以上にある 4,200 以上のエッジ PoP で構成される、世界で最も分散されたクラウドプラットフォームを構築しました。

Akamai のお客様には、証券会社のトップ 10 社、銀行のトップ 10 行、動画ストリーミングサービスのトップ 10 社、ビデオゲーム企業のトップ 10 社がすべて含まれています。Akamai の顧客基盤は、ほとんどの大手自動車会社、ヘルスケア提供機関、小売企業、通信事業者から、数多くの行政機関や軍事機関まで、多岐にわたります。

お客様から信頼を寄せていただいているのは、Akamai がお客様の力となり、守っているからです。Akamai は、1 日あたり 400 億のボット、1 日あたり 7 億 8,000 万件のアプリケーション攻撃、1 四半期あたり 1,889 件の DDoS 攻撃によるネットワーク停止の危機からお客様を保護しています。1 社のお客様から得られた脅威インテリジェンスを活用し、すべてのお客様に保護を適用することで、Akamai はセキュリティを提供します。Akamai のグローバルプラットフォームの規模は、AI 時代に移行する組織のセキュリティを確保するために必要なデータ量と品質の両方をもたらします。

グローバルな拡張性

WAF における拡張性の問題は、Web トラフィックの必要な量（最初の量と徐々に増加する量）と、トラフィックの評価に必要な WAF ルールの数の両方を検査する能力が中心となっています。従来のハードウェアベースの WAF ソリューションは、多くの場合、拡張性が不十分です。これは、それらのソリューションがアプライアンス内で使用できる CPU とメモリーリソースに制限され、同一アプライアンス上で他のソリューションと競い合う必要があるためです。

Akamai のクラウドプラットフォームに統合型の WAAP ソリューションを展開すれば、Akamai の分散型サーバーリソースを活用して受信した Web トラフィックを検査できるため、拡張性の問題が解消します。ユーザーと攻撃者は、最も近い Akamai サーバー経由で保護された Web サイトに接続し、そのサーバーが攻撃者のトラフィックを検査して、検知された悪性のリクエストをブロックします。これにより、Akamai の WAAP ソリューションを使用すれば、Web アプリケーションのトラフィック量の増加（トラフィックの急激な増加と長期的な増加の両方）に加え、世界中の新規ユーザーの所在地に合わせてシームレスに拡張できます。

パフォーマンス

パフォーマンスが悪い場合、セキュリティソリューションの展開、特にアプリケーションの前にインラインで展開される WAAP ソリューションの妨げになる可能性があります。ビジネスに不可欠な Web サイトのパフォーマンスが低下すると、生産性の低下、質の低いユーザー体験、市場投入までの時間の延長、収益の減少につながりかねません。

世界規模の Akamai のクラウドプラットフォームを使用すれば、パフォーマンスを低下させることなく、WAAP で Web アプリケーションを保護できます。グローバル分散型の WAAP は、プラットフォームで最初に受信した HTTP トラフィックを検査し、プラットフォーム上のすべてのサーバーのトラフィックの検査に必要な CPU とメモリーリソースを分配します。そのため、組織内の障壁や展開の妨げの元となるパフォーマンスの問題が解消します。

エッジプラットフォームによる保護の強化

クラウドに依存しない Akamai の Web アプリケーション・セキュリティ・ソリューションは、プラットフォーム全体でシームレスに機能し、幅広いアプリケーション攻撃や API ベースの攻撃を防ぎます。次の図は、正規ユーザーのパフォーマンスとアクセスを向上させながら、脅威をオリジンから遠ざけるために使用される、Akamai の多層的なセキュリティメカニズムと制御機能の全容を示しています。

App & API Protector には、すぐに利用できる包括的な防御を実現するために、さまざまなセキュリティメカニズムと制御機能が自動的に組み込まれています（青色で表示）。他の Akamai 製品やサービスを追加することで、レイヤー 7 の完全な保護が実現します

攻撃に対するマネージドサポート

Akamai は、継続的な WAAP 管理に加え、攻撃に対するマネージドサポートをお客様に提供しています。これは、保護されている Web サイトを 24 時間体制で監視し、検知された攻撃への対応を管理するものです。

攻撃に対するマネージドサポートでは、Akamai の世界中の SOC のスタッフを活用し、セキュリティインシデントの発生に次のように対応します。

- WAAP アラートとお客様のリクエストに対応し、その後の問題の調査を実施します
- 適切な攻撃の特徴を判断し、追加の緩和策を展開します
- カスタマー・アプリケーション・チームと協力して、展開された緩和策の効果と正確さを測定し、必要に応じて緩和策を調整します
- インシデントの発生後、カスタマー・アプリケーション・チームとともに対応全体を確認します
- インターフェース内で、緊急サポートを要請するための攻撃アラートボタンを提供します

Security Operations Command Center（SOCC）

Akamai の SOCC は、10 年以上にわたり世界最大規模の攻撃の多くを緩和するのに貢献し、進化を続けるグローバルな脅威からお客様を保護してきました。

悪性攻撃の監視と緩和には、次の 4 つの機能が必要です。

- グローバルな可視性
- プロアクティブな監視とアラート
- アジャイルな攻撃緩和
- 経験豊富なセキュリティチームによる継続的なアドバイザリーサービス

Akamai SOCC は、世界最大規模のセキュリティインフラを運用することで、これらの機能を提供します。すべてのネットワークトラフィックが Akamai の統合セキュリティプラットフォームで実行され、リアルタイムでインテリジェンスが収集されます。たとえば、Akamai は最近の SQL インジェクション攻撃の大幅な増加などのセキュリティトレンドを収集しました。

これにより、Akamai のセキュリティチームは、効果を最大限に高め、影響を最小限に抑えながら、お客様の脅威を迅速に緩和できます。

結論

API やクライアントサイドのコンポーネントを介した新しい形態の自動ボットや標的型攻撃が登場したため、組織はネットワークレイヤーやアプリケーションレイヤーの DDoS からの保護だけでなく、包括的な多層防御のセキュリティアプローチによってすべての Web アプリケーション、API エンドポイント、ブラウザー、インフラを保護しなければならなくなりました。セキュリティのリーダーや専門家は、複数の攻撃ベクトルからの脅威を迅速に特定して緩和し、ファイアウォールを越えて隣接するセキュリティテクノロジーへ従来の保護を拡張し、最高のセキュリティ防御を実現する Web アプリケーションセキュリティを必要としています。

WAAP に対する Akamai のアプローチは、現代のセキュリティポスチャに必要なすべてのセキュリティテクノロジーを備えることによって比類のない幅広さと有効性を実現したソリューションセットを提供することです。Akamai は、トップクラスのセキュリティソリューションは世界最大規模のブランドや大人気のブランドだけを対象としたものであってはならないと考えています。アプリと API 保護のための Akamai のポートフォリオは、多層的なポートフォリオを通じて、セキュリティ第一のあらゆる組織が効果的な Web アプリセキュリティを利用できるようにします。

継続的に進化して適応し、深く広範な攻撃インテリジェンスを活用するセキュリティソリューションを提供する Akamai は、グローバル企業と提携し、セキュリティの最新化と継続的な改善を実現しています。インテリジェンス、可視性、自動化、内部の取り組みを推進するためのガイダンスを組織のセキュリティチームに提供すると同時に、企業システムから攻撃者を排除することを目指しています。そのため、Akamai はオンラインライフのカとなる極めて要求の厳しいブランドの保護を任されています。

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X と LinkedIn で Akamai Technologies をフォローしてください。公開日：2025 年 2 月。