AKAMAI 製品概要

App & API Protector

今日のコネクテッドワールド（つながった世界）では、新たな脅威や進化する脅威など、さまざまな脅威から Web アプリケーションおよび API を守ることが、ビジネスの成功を左右する重要な要件となっています。しかし、クラウドへの移行や最新の DevOps 手法の導入が進み、アプリケーションが絶えず変化する状況でデジタルインタラクションのセキュリティを確保するためには、新たな複雑さや課題に対応しなければなりません。

包括的な Web アプリケーションおよび API 保護（WAAP）ソリューションを導入することで、変化に合わせて保護機能を更新し、標的となる脆弱性に対する知見をいち早く把握し、セキュリティ対策を強化できます。

Akamai App & API Protector は、Web アプリケーションファイアウォール（WAF）、ボット緩和、API 保護、分散型サービス妨害（DDoS）防御など、多くのセキュリティテクノロジーを 1 つのソリューションに統合しています。App & API Protector は、従来の WAF よりも脅威をすばやく特定して緩和し、デジタル資産全体を多元的な攻撃から守る、先進的な WAAP ソリューションとして評価されています。導入が容易で、使いやすく、総合的な可視性を提供するプラットフォームは、Akamai Adaptive Security Engine を使って最新のカスタマイズされた保護を自動的に実装します。

適応型セキュリティの力

App & API Protector はルールセットを超えた機能、Adaptive Security Engine を備えています。この革新的なテクノロジーにより、セキュリティ保護機能は継続的かつ自動的に更新され、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ます。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、そして 400 人を超えるセキュリティ専門家と脅威研究者の知見を組み合わせて、最先端の保護を実現します。Adaptive Security Engine には、次のような独自性があります。

- あらゆるリクエストの特性をエッジでリアルタイム分析し、迅速に検知
- ローカルおよびグローバルデータを使用して攻撃パターンを学習し、お客様に合わせて防御手法を調整
- 将来の脅威に適応し、攻撃が進化しても保護を確実に更新

Adaptive Security Engine は、ゼロタッチ更新やほぼ無干渉の更新で、時間のかかる手動調整の負担を軽減します。提供開始時点で、このテクノロジーによって検知数が 2 倍に増加し、フォールスポジティブ（誤検知）の発生数が 5 分の 1 に減少することが実証されています。機械学習アルゴリズムの最新の更新により、現在では誤検知がさらに 4 分の 1 に減少しました。セキュリティ担当者は本来の能力を発揮できるようになり、セキュリティの確保とお客様重視のデジタルビジネス運営に専念できます。

ビジネス上のメリット

信頼できる攻撃検知
脅威環境の進化に伴い、DDoS、ボットネット、インジェクション、アプリケーションおよび API 攻撃など、既知の攻撃や新たな攻撃を阻止します。

ひとつの製品で広範な防御機能
WAAP、ボットの可視化と緩和、DDoS 防御、セキュリティ情報およびイベント管理（SIEM）コネクター、Web 最適化、クラウドコンピューティング、API アクセラレーションなどの機能を持つソリューションを使用することで、セキュリティへの投資を最大限に活用できます。

ハンズオフセキュリティ
Akamai Adaptive Security Engine を活用した自動更新とプロアクティブなセルフチューニングの推奨により、時間のかかる手動メンテナンスの負担を軽減します。

使いやすさ
改善された UI デザインを利用して、オンボーディングと包括的なセキュリティ運営をシンプル化できます。セットアップおよびトラブルシューティングガイドも効果的です。

総合的な可視性
Akamai のセキュリティソリューションの共有テレメトリーを使用して、単一のダッシュボードやプロアクティブな探索レポートでセキュリティ指標の全容を分析できます。

新機能：Behavioral DDoS Engine

機械学習を活用した新しい Behavioral DDoS Engine（ふるまい DDoS エンジン）は、アプリケーションレイヤーの DDoS 防御の強化とシンプル化の両方を行います。Behavioral DDoS Engine のふるまいベースおよび異常ベースの検知アルゴリズムは、発信元の国、ネットワークフィンガープリント、その他の HTTPS リクエスト属性など、さまざまなトラフィックディメンションを調べて、カスタマイズされた保護を構築し、アプリケーションレイヤーの DDoS 攻撃に対処する負担を軽減します。

Behavioral DDoS Engine は、機械学習を利用することにより、有効性と、トラフィックプロファイルやベースラインの作成に使用するトラフィックディメンションに関する意思決定を向上させます。さまざまな感度レベルに対するスコアリングメカニズムでは、攻撃の検知と誤検知の最小化に関する企業のリスク選好が考慮されます。

ルールセットを超えて進化した Akamai App & API Protector は、Adaptive Security Engine によって強化されています。

先進的な攻撃検知 — デジタル環境の発展に合わせて、Akamai のお客様の保護の幅が広がり、その深さも増しています。Adaptive Security Engine による自動更新と適合型の自動調整に加えて、App & API Protector は、アナリストが認める高度な検知機能により、DDoS、ボット、マルウェア、その他の攻撃ベクトルを明らかにします。Akamai の脅威調査ツールを使用して、新たな CVE や進化する CVE に対抗する Akamai の保護機能をご確認ください。

アプリケーションセキュリティ — App & API Protector は、組織のニーズに合わせてセキュリティを調整できるように、一連の防御機能とカスタマイズ機能を完備しています。Client Reputation、ネットワークリスト、新たな攻撃の検知などの効果的な機能により、セキュリティ運営をシンプル化しながら、攻撃者に対する優位性を確保できます。Akamai WAAP ソリューションの高度なアプリケーションレイヤー防御機能は、DDoS、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、サーバーサイド・リクエスト・フォージェリー、その他の攻撃ベクトルに対抗します。

DDoS 防御ときめ細かいレート制御 — 市場をリードする DDoS ソリューションとして評価されている App & API Protector は、複数の前線で DDoS 防御を提供します。まず、ネットワークレイヤーの DDoS 攻撃を即座にエッジにドロップすることにより、リスクを緩和し、リソースを節約します。続いて、高度なレイヤー 7 DDoS 攻撃をエッジで自動的に検知して緩和し、進化し続ける DDoS 脅威に対する負担の少ないリアルタイムの防御を実現します。きめ細かいレート制御により、トラフィックプロファイルと攻撃プロファイルに合わせて DDoS 防御をカスタマイズできます。

ボットの可視化と緩和 — 1,750 を超える既知のボットから成る Akamai の広範なディレクトリにアクセスすることで、ボットトラフィックをリアルタイムで可視化できます。また、歪められてしまった Web 分析を調査したり、オリジンの過負荷を防いだりするほか、独自のボット定義を作成して、サードパーティやパートナーのボットが阻止されずにアクセスできるようにすることも可能です。現在では、ブラウザーなりすましの検知、条件付きアクション、クリプトチャレンジなど、App & API Protector のボット制御が拡張されています。

OWASP Top 10

Akamai は OWASP Top 10 と OWASP API Security Top 10 の両方のリスクを緩和します。App & API Protector と Akamai のセキュリティ機能がお客様を大規模な脅威や一般的な脅威、新たな脅威からどのように保護しているのかご覧ください。

OWASP Top 10 に対する Akamai の防御について、詳しくはホワイトペーパーをダウンロードしてご確認ください。

API 保護 — 業界をリードする Akamai の API 保護は、デジタル資産全体のトラフィックを可視化し、脆弱性をいち早く明らかにし、環境的な変化を特定し、隠れた攻撃を防御することで、セキュリティを強化します。App & API Protector の API 機能を使用することで、次のことを行えます。

- エンドポイント、定義、トラフィックプロファイルなど、Web トラフィック全体の API を自動探索。既知の API に加え、未知の API や変更された API もすべて探索
- 数回クリックするだけで、新たに発見された API を簡単に登録可能
- DDoS 攻撃、悪性のインジェクション攻撃、Credential Abuse 攻撃、および API 仕様違反に対する API 防御を確保
- App & API Protector の個人を特定できる情報の報告機能により、機微な情報を管理し、コンプライアンスを維持

最大規模のグローバルネットワークが提供するパフォーマンスとその他のメリット — Akamai プラットフォームをご活用いただくことで、お客様は、比類のないグローバル規模のスケールによる競争優位性を獲得し、世界のインターネットトラフィックの大部分をリアルタイムで可視化することができます。この膨大なデータにより、Akamai は、実用的な脅威インテリジェンスを提供し、組織が進化するセキュリティ脅威に先手を打ち、さまざまな環境での迅速な攻撃の検知と緩和を実現するための支援を、提供することができます。また、確かなパフォーマンス向上を実現し、100% の可用性 SLA を保証します。

Malware protector — このアドオンモジュールは、ファイルがアップロードされる前にエッジでスキャンし、マルウェアが悪性のファイルアップロードとして社内システムに侵入するのを検知して防ぎます。追加のアプリや API 設定は不要で、システムごとに保護を個別に設定する必要もありません。

Simple Start オンボーディング — 優れたセキュリティツールも、使用できなければその効果を発揮しません。Akamai は使いやすいプラットフォームの構築に取り組み、生産性と強力な保護機能の実現に注力しています。お客様は Akamai の Simple Start を使用して迅速にオンボーディングしたり、わずか数回のクリックで新しいアプリケーションに保護を適用したりできます。

ダッシュボード、アラート、レポート作成ツール — Web Security Analytics は、Akamai の詳細な攻撃テレメトリーダッシュボードです。ここでは、セキュリティイベントを分析できます。また、静的フィルターとしきい値を使用してリアルタイム E メールアラートを作成できるほか、Akamai プラットフォーム全体の保護の有効性を継続的に監視し評価するためのカスタマイズ可能なレポートツールも使用できます。

DevOps の統合 — GitOps を使用してセキュリティを DevOps ワークフローにシームレスに統合し、ハイペースな開発と足並みの揃ったセキュリティを実現することができます。CLI または Terraform から利用できる Akamai の API により、コードを介して App & API Protector を完全に管理し、ユーザーインターフェースで利用可能なすべてのアクションを調和させることができます。

SIEM 統合 — SIEM の API にも対応しています。Splunk、QRadar、ArcSight などに事前に組み込まれているコネクターは、App & API Protector に自動的に組み入れられます。

組み込まれている機能 — 可視性とパフォーマンスを高めるために、App & API Protector は、Akamai のお客様から高い評価を得ている以下のような多くの製品を搭載しています。

- Site Shield：攻撃者がクラウドベースの防御を迂回しオリジンインフラを狙うのを防ぐ
- mPulse Lite：ユーザーのふるまいを詳細に可視化し、リアルタイムのパフォーマンス問題に対応し、デジタル変化による収益への影響を測定
- EdgeWorkers：市場投入までの時間を短縮し、エンドユーザーに最も近い場所でロジックを実行するなど、サーバーレスコンピューティングならではの強みを提供
- Image & Video Manager：品質、形式、サイズの最適な組み合わせにより、画像と動画の両方をインテリジェントに最適化
- API Acceleration：容易なアクセス管理、需要の急増に合わせたスケーリング、API セキュリティの強化により、API パフォーマンスを飛躍的に向上

無料枠の特典は使用に際して制限がある場合があります。詳細については、Akamai までお問い合わせください。

Advanced Security Management

オプションの Advanced Security Management モジュールは、より複雑なアプリケーション環境や高度なセキュリティニーズを持つお客様に、自動化と設定の柔軟性を提供します。Advanced Security Management オプションには、すぐに使える機能として、追加のセキュリティ設定、レートポリシー、セキュリティポリシー、アプリケーションレイヤー DDoS 制御、カスタム WAF ルール、ポジティブ API セキュリティ、および IP レピュテーション脅威インテリジェンス（Client Reputation）へのアクセスが含まれます。

Managed Security Service

標準サポートは、すべての Akamai のお客様に 24 時間体制で提供されます。コンサルティングまたは単一プロジェクト案件のオンデマンドのプロフェッショナルサービスに加えて、Akamai は、完全マネージド型 WAAP サービス、マネージド型攻撃サポート、専門的なセキュリティ・オペレーション・センターのサポートという、レベル別のマネージド型サービスを提供します。

App & API Protector の詳細や無料トライアルのお申し込みについては、akamai.com/aap をご覧ください。