WEB アプリケーションと API の保護性能：

金融機関向けチェックリスト

アプリケーション・プログラミング・インターフェース（API）は、あらゆる種類のデバイス、アプリケーション、データ間の相互接続をサポートする大きな可能性と能力を備えており、銀行内外の幅広い戦略と活動を支えるテクノロジーです。API は、オープン性が高まる可能性を秘めており、競争力を高め顧客に利益をもたらすことができます。しかし、金融サービス業界での API 使用が急速に増えたことで、アタックサーフェスが拡大し、新たなセキュリティリスクが発生しています。

情報セキュリティ戦略の計画、実装、最適化の一環として、Web アプリケーションと API のセキュリティソリューションを組み込むことは、貴社に固有のリスクを把握し、セキュリティギャップに的を絞って、脅威を検知することにつながります。金融機関が競争力を維持するためには、包括的な知見と継続的な可視性、および最も巧妙な攻撃を特定して阻止できる機能を備えた Web アプリケーションと API 保護（WAAP）ソリューションが必要です。

このチェックリストは、ベンダーの機能の評価に加え、効果的な WAAP ソリューションの実装に必要な要件のリストとしても使用いただけます。

01. プラットフォーム要件

02. 適応型の Web アプリケーション保護と DDoS 防御

03. API の可視性、保護、制御

04. 柔軟な管理

01 プラットフォーム要件

- パフォーマンスを損なわずに、トラフィック需要に応じて常に保護を提供できるスケーラビリティ
- 地理的に分散したアプリケーションに対応できるアーキテクチャ
- 適切に使用されていることを確認できる監査ログ機能
- オンプレミス、プライベート、パブリッククラウド（マルチクラウド、ハイブリッドクラウドを含む）のサイトオリジンの保護
- ネットワークレイヤー［L3/L4］の分散型サービス妨害（DDoS）緩和に関するゼロ秒 SLA（サービスレベル契約）
- プラットフォーム全体にわたるクラウドソースの攻撃インテリジェンスにより、攻撃者、攻撃頻度、攻撃の重大度を特定できる可視性
- ポート 80 とポート 443 経由の Web トラフィックのリバースプロキシ
- SSL／TLS　暗号化によるネットワークプライバシー保護
- 少なくとも 5 年間の、公平な第三者による、ソリューションカテゴリー内での実績あるリーダーとしての認定
- 個人を特定できる情報（PII）がいつ、どこで送信されるかを自動的に検出して警告し、データ漏洩を防止する機能

金融機関には、機微な顧客情報や財務上のデータを、急速に進化するセキュリティ脅威から守る責任があります。これに対応するためには、Web アプリケーション・セキュリティ・ソリューションは、柔軟でスケーラブル、かつ容易に管理できるものである必要があります。

適応型の WEB アプリケーション保護と DDoS 防御 02

最も正確で信頼性の高いセキュリティを実現するためには、Web アプリケーションセキュリティは、従来のシグネチャベースの検知ではなく、より高度な適応型の Web アプリケーション保護と DDoS 防御へと進化する必要があります。

- 異常スコアリングやリスクベースのスコアリングによる、シグネチャベースの攻撃検知を超える検知
- 継続的な設定と更新が不要な、フルマネージド型の WAF ルール
- 個々および共有の IP アドレスに対応する、クライアント・レピュテーション・スコアとインテリジェンス
- 機械学習、データマイニング、ヒューリスティック分析に基づいて、急速に進化する脅威を特定
- セキュリティリサーチャーが提供する継続的なリアルタイム脅威インテリジェンスによる Web Application Firewall（WAF）ルールの自動更新
- 本番環境に展開する前に、ライブトラフィックに対して新規または更新された WAF ルールをテストする機能
- SQL インジェクション、XSS、ファイルインクルージョン、コマンドインジェクション、SSRF、SSI、XXE に対する防御（最小限）
- 顧客の要件に合わせてカスタマイズ可能な事前定義済みルール
- 再帰的なアプリケーションアクティビティにより Web サーバーに過負荷を与えるよう設計されたアプリケーションレイヤー［L7］ボリューム DoS 攻撃からの防御
- 特定のトラフィックパターンに対して迅速に保護を提供するカスタムルール（仮想パッチ）
- 自動化されたボットトラフィックや過度なボットトラフィックを防ぐためのリクエスト制限
- オリジンを標的にした直接攻撃からの防御
- 特定の IP、サブネット、地域からのトラフィックをブロックまたは許可する、複数のネットワークリストを介した IP／地理制御
- 脆弱性スキャンや Web 攻撃ツールなど、自動化されたクライアントからの防御

03

APIの可視性、保護、制御

- 未知の API や変化する API（API エンドポイント、特性、定義など）の自動検出とプロファイリング
- API ベースの攻撃を検知するための XML リクエストと JSON リクエストの自動検査
- API キーに基づく API エンドポイントのレートコントロール（スロットリング）
- IP／地域に基づく API ネットワークリスト（許可リスト／ブロックリスト）
- バージョン管理による API ライフサイクル管理
- 特定のユーザー要件を満たすカスタム API 検査ルール
- JSON Web Token（JWT）の検証による安全な認証と認可
- 許容できる XML と JSON オブジェクトフォーマットを事前定義し、API リクエストのサイズ、タイプ、深さを制限する機能
- リソースを枯渇させるよう設計された Low & Slow（少しずつ時間をかけた）攻撃（Slow Post、Slow Get など）から、API バックエンドのインフラを保護
- 許可される API リクエストをキーごとに定義（各キーに対する割り当ては個別に定義）し、消費を完全制御
- 標準 API 定義を使用した API オンボーディング（Swagger／OAS および RAML）
- API レベルでのリアルタイムのアラート、レポート、ダッシュボード

API 保護は、Web アプリケーションセキュリティの重要な要素となっています。API の脆弱性を緩和し、リスクサーフェスを縮小するためには、強力な API 検知、保護、および制御機能を備えた WAAP ソリューションが必要です。

Akamai

柔軟な管理

04

- セキュリティ設定タスクを CI／CD プロセスに統合するための Open API と CLI
- リアルタイムのダッシュボード機能、レポート機能、ヒューリスティック分析に基づくアラート機能
- オンプレミスおよびクラウドベースのセキュリティ情報やイベント管理（SIEM）アプリケーションとの統合
- 詳細な攻撃テレメトリーへのアクセスとセキュリティイベントの分析ができる、集中型ユーザーインターフェース（UI）
- 完全なステージング環境と変更管理を実装する機能
- トラフィックに自動的に適応する、自己調節型のセキュリティ保護
- セキュリティ管理、監視、脅威の緩和をオフロードまたは強化できる、フルマネージド型セキュリティサービス

投資効果を最大化し、運用効率を上げるためには、シンプルで自動化されたワークフローが必要です。新しいアプリケーションや変更するアプリケーションの保護、新しい WAF ルールの導入、API への保護の拡大。どの場合でも、プロセスはシームレスかつ直感的である必要があります。

Akamai は、世界中の大手金融機関に Web アプリケーションと API 保護を提供しています。当社のグローバル・セキュリティ・リサーチ・チームは毎日、数百万件もの Web アプリケーション攻撃、数十億件のボットリクエスト、数兆件の API リクエストから得た知見を収集しています。収集した知見を高度な機械学習や脅威リサーチと組み合わせることで、継続的な改善、新たな脅威の発見、革新的な機能の開発が可能になります。

Akamai の Web アプリケーションと API セキュリティソリューションは、最先端の Web アプリケーション攻撃、DDoS 攻撃、API ベースの攻撃から金融機関を保護します。最新の Akamai リサーチは、セキュリティハブでご確認いただけます。今後も引き続きご注目ください。