究極の WAF 評価チェックリスト

アプリケーションと API のセキュリティニーズに最適なソリューションを見つけるためのツール

Web アプリケーションファイアウォール（WAF）や、Web アプリケーションと API の保護（WAAP）の適切なベンダーを、シンプルに探索できます。この包括的なチェックリストを、WAF と WAAP プロバイダーの評価にご活用ください。そのソリューションが、セキュリティ、パフォーマンス、財務、運用のニーズを満たしているかどうかをご確認いただけます。

セキュリティ機能

アプリケーションセキュリティ

- **OWASP Top 10 の脆弱性**（SQL インジェクション、XSS、LFI、SSRF など）**に対応している**ことを確認します。保護をカスタマイズして自動的に展開できるかどうかを確認します。
- **評判の悪い IP** からのトラフィックをプロアクティブに制御し、従来の**例外が悪用されている**場合は警告するソリューションであるかどうかを評価します。
- **許可リストとブロックリストの柔軟性**を評価します ― IP、地域、ASN、TLS フィンガープリントなどの属性を関連付けて、効果的なポリシーを作成できるでしょうか？

DDoS 防御

- ベンダーが、DNS、レイヤー 3 および 4、レイヤー 7 を含むアプリケーションと API に対して**マルチレイヤー DDoS 防御**を提供していることを検証します。
- そのソリューションがアプリケーションセキュリティ向上のために**ふるまい DDoS 検知**を提供していることを確認します。
- **レート制限**の粒度を判断します。設定は自動でしょうか、手動でしょうか？これらの対策によって、ボリューム型攻撃とスローポスト攻撃の両方から保護できるでしょうか？
- DDoS 攻撃時の**負荷を軽減**し、パフォーマンスを強化する機能を確認します。
- DDoS 攻撃時のトラフィック増加による潜在的な**追加コスト**について把握します。
- **L7 DDoS 防御が自動化**されており、チームの時間と専門知識の浪費を防げることを確認します。こうした**保護**は、特定のトラフィックプロファイルやリスク許容度に**適応**していますか？

ゼロデイ攻撃に対する防御

- WAF が、**既知の CVE に対する既存の保護機能**を備えており、新しいゼロデイ攻撃から防御するために迅速に調整できることを確認します。ソリューションの**ゼロデイ防御に関する実績**と応答時間を調査します。
- 顧客として、**特定の CVE に対する保護**を備えているかどうかを判断します。

API 保護

- インジェクション攻撃、DoS、仕様違反から **API エンドポイントを保護**するソリューションであることを確認します。
- **API 探索**の確認 — 新しい API や変更された API を自動的に検知できますか？どの程度簡単に保護を適用できますか？
- **PII の検知とアラート**を確認して、機微な情報を保護し、データ漏えいを防止します。

ボットからの防御

- WAF がボットディレクトリと定義を使用して、**自動化された脅威を検知し、緩和する**かどうかを確認します。ボットディレクトリの拡張性はどの程度ですか？新しいボットや変更されたボットでどの程度頻繁に更新されますか？
- ツールに存在する**ボット定義**を判断します。**独自の**ボット定義を**作成**できますか？
- ソリューションに、ユーザー体験を妨げない **CAPTCHA または人間による検証メカニズム**が含まれているか確認します。エンドユーザーが先に進む前に、CAPTCHA や検証とのやり取りが求められますか？

脅威インテリジェンスと自動化

脅威インテリジェンス

- プロバイダーが、脅威インテリジェンスに関して**ファーストパーティのデータ**を使用し、サードパーティによる遅延やデータ改ざんの可能性を回避していることを確認します。
- プロバイダーの**脅威ハンティングチームの規模**と、新たなリスクを監視するセキュリティエキスパートのグローバルネットワークを検証します。
- インテリジェンスデータベースで処理される**データの量と関連性**を評価します。自社に類似した業界のデータや、サイバー攻撃の標的になりやすい組織のデータが含まれていますか？

自動化

- WAF が**古いルールセットテクノロジー**に依存しているかどうかを確認します。先進的なヒューリスティックや機械学習による自動更新など、高度で最新のテクノロジーを使用していますか？
- ルールセットが自動的に更新され、**手動での操作が不要になる**ことを確認します。自動更新はグローバルなレベルで適用されますか？前に適用した更新を削除したり、**ライブトラフィックでテスト**したりするために、どのようなオプションが可能でしょうか？
- 自社の環境に合わせて保護をカスタマイズする際に作業を必要としないソリューションであるかどうかを判断します。そのソリューションは、組織のライブトラフィックのプロファイルに基づいてセキュリティポリシーを継続的に**自動調整**していますか？
- ソリューションが**フォールス・ポジティブ（誤検知）**を制御する方法を評価します。誤検知の削減と、**有効なトラフィックの中断**の最小化をどのように両立させているでしょうか？

可視化とレポート

きめ細かい可視性

- WAF が、複数のソリューション環境に対応するカスタマイズ可能なダッシュボードとレポート機能を備え、**脅威**とパフォーマンスを**詳細に可視化**することを確認します。
- WAF の運用において、セキュリティチームはほとんどの時間をデータコンソールの使用に費やします。**カスタマイズ**、プロアクティブな分析、**レポートの粒度**について、どのような機能が利用可能になるか調査します。
- ソリューションが、**API トラフィック**とアプリケーショントラフィックを効果的に**監視**し、不正使用を検知し、API の無秩序な拡大に関する、詳細な知見を提供する能力を評価します。

リアルタイムのアラートとプロアクティブな分析

- 重要な脅威についてチームに知らせる、ほぼ**リアルタイムのアラート機能**を備えているか確認します。アラートは、理解しやすく迅速に対応できるように、影響度、ソース、攻撃タイプなどの特定の基準に基づいてカスタマイズする必要があります。
- 攻撃が発生する場所、タイミング、方法について**分析済みの知見**を提供し、セキュリティチームの負担を軽減するソリューションを探します。セキュリティ状況を改善するための**次の手順を提案する**機能も必要です。

プラットフォームとアーキテクチャ

グローバルなリーチ

- WAF がグローバルネットワークのエッジまたは CDN サービスへのアクセスを提供し、パフォーマンスとセキュリティを強化するかどうかを確認します。ソリューションの**グローバルな可用性**を調査して、自社と顧客にとって主要な場所がカバーされていることを確認します。

クラウドとハイブリッドのサポート

- ソリューションが**クラウドに依存せず**、マルチクラウド、ハイブリッド、オンプレミスの各環境をサポートできることを確認します。CDN ベースの場合は、そのソリューションが CDN を超えて保護を拡張し、エッジ外のセキュリティを確保できることを確認します。

回復力とフェイルオーバー

- **ソリューションの回復力**を評価します。— 機能停止や中断が発生しても、フェイルオーバーを自動的に実行して保護を維持できるでしょうか？
- プロバイダーの、**最近発生したサービスの中断と対応**について確認します。
- **サービスレベル契約**（SLA）がビジネスニーズを満たしているかどうかを判断します。

サポートとマネージドサービス

含まれているサポートとサービスへのアクセス

- WAF ソリューションに**含まれるサポートレベル**と、有料で利用可能なサポートレベルについて判断します。
- **24 時間**体制**のインシデント対応**が可能かどうか、また攻撃を受けている最中にセキュリティ・オペレーション・センター（SOC）に直接問い合わせできるかどうかを確認します。
- 攻撃や設定のための専門知識や、スタッフの異動に対処する、社内リソースの潜在的なギャップに対応するために、ベンダーが**完全なマネージド・セキュリティ・サービス**を提供するか確認します。

統合と DevSecOps の互換性

API、CLI、インフラの自動化

- **API、CLI、Terraform** の統合を確認して、セキュリティの自動化と開発ワークフローへの組み込みを実現します。GitOps、およびその他の Infrastructure as Code（コードとしてのインフラ）フレームワークのサポートは、環境全体での一貫したセキュリティ適用のために不可欠です。

SIEM 統合

- WAF が、Splunk や QRadar などの **SIEM ツールとシームレスに統合され**、監視、レポート、インシデント対応を強化しているか確認します。

ビジネスの成果と効率性

スケーラビリティとパフォーマンス

- パフォーマンスを低下させることなく大量のトラフィックを処理するために、ソリューションが**自動スケーリング**可能であることを確認します。そのソリューションは、どの時点でレイテンシーが発生したり、大きな負荷に対して脆弱になったりするでしょうか？
- **100% の可用性**を保証する SLA であることを確認し、ソリューションが、キャッシングやトラフィック高速化などのパフォーマンス強化機能を提供して、アプリケーションを改善できるかどうかを評価します。

統合管理

- プロバイダーが、クラウド、オンプレミス、ハイブリッドなど、**すべての環境でセキュリティポリシーを管理できる**単一画面のインターフェースを提供しているか、評価します。ソリューションが現在のスタックと統合可能であり、セキュリティチームと開発チームの両方にスムーズな体験を提供することを確認します。

優れたコスト効率

- ソリューションについて、**WAF、DDoS、ボット管理、API 保護を**単一ベンダーに**統合**する能力があるか評価し、複雑性と管理コストの削減を図ります。セキュリティの有効性と運用コストのバランスを評価し、全体的な価値を判断します。

信用とベンダーの信頼性

サービスと安定性の履歴

- 過去 5 年間における、プロバイダーの**停止およびサービスの中断に関する履歴**を確認します。
- **財務的に安定している**会社であることを確認します。収益性は高いでしょうか？いつから事業を展開しているでしょうか？どのような規模と種類の顧客に対応していますか？

評判とレビュー

- 検証済みのレビューと顧客の声を調査し、同じ業界の類似した組織が**そのベンダーを信頼しているかどうかを**確認します。現在の顧客のユースケースは、自社のニーズに合っていますか？
- Gartner や Forrester などの**業界アナリストが**、アプリケーションおよび API 保護ソリューションについて評価しているかどうかを確認します。
- ベンダーとの話し合いの後で、顧客になって問題が発生した際はそのベンダーの対応とサポートに**自信を持てると感じられるか**、確認します。最初のオンボーディング後に、誰が担当者となるかを質問します。

Akamai の WAAP ソリューションの詳細については、
App & API Protector の無料トライアルをぜひお試しください。

 | サポート | | 公開日：2024 年 12 月