ORACLE®
Cloud Infrastructure

Oracle Cloud Infrastructure Web Application Firewall

課題

Webアプリケーションのセキュリティついて、企業の関心が高まっています。あらゆるサイバー攻撃のうち、かなりの割合がWebアプリケーションを対象としており、その割合は増加しています。

クラウド・コンピューティングの増加、オープンソース・テクノロジーの利用、データ処理要件の増加、Webアプリケーションの複雑化、そして攻撃者の全体的能力の拡大といった要因が、ITセキュリティ責任者にとって非常に厳しい環境をもたらしています。

侵害が発生しても、その多くは回避できたかもしれません。ところが、セキュリティ予算が追いついていないのです。情報テクノロジーのリーダーたちは、イノベーションはもちろん、侵害の緩和、回避、侵害後の修正、クリーンアップのためのコスト拡大に追従しようと苦労しています。

ご存知でしたか

すべてのクラウド*WAF*ソリューションが同じように構築されているわけではありません。多くのプロバイダは、パブリック・クラウド・ハイパーバイザ・サービスで実行される仮想マシン（*VM*）として*WAF*を提供しています。ところが、クラウドベースの*VM*は、顧客がパッチを適用したり、アップデートしたりしなければなりません。
顧客は、使用する*VM*のスケーリングを担うことになりますが、クラウドネイティブの*WAF*はスケーリングできるよう構築されています。*WAF*を評価する場合は、グローバルなクラウド・インフラストラクチャにサポートされている、純粋なクラウドベースのソリューションをご検討ください。

Oracle Cloud Infrastructure Web Application Firewall：グローバルに分散したクラウドベース・ネットワーク

よかれと思って構築したセキュリティ制御も、サイバー攻撃者がグローバル・ネットワークを利用でき、攻撃の場所を継続的に変えることができる場合は、企業のセキュリティにおける弱点となることが少なくありません。

最終的に、サイバー犯罪者は境界しかない組織の防御を混乱させたり、侵害したりします。企業の防御を拡張するため、グローバルなセキュリティ・プラットフォームが求められています。企業は、攻撃を阻止するスタート地点として、グローバルにスケーラブルで分散したソリューションを採用しなければなりません。

Oracle Cloud Infrastructure（OCI）Web Application Firewall（WAF）は、グローバルに展開された、エンタープライズ・グレードのクラウドベース・セキュリティ・ソリューションで、今日のWebアプリケーションが抱える課題に対処するよう設計されています。OCI WAFは、サイバー攻撃からWebアプリケーションを保護する、レイヤー化された手法を用いたセキュリティ・サービスのスイートを提供します。

OCI WAFが提供する内容

OCI WAFは、グローバルに展開された、エンタープライズ・グレードのクラウドベース・セキュリティ・ソリューションで、ビジネス・クリティカルなWebアプリケーションを悪意あるサイバー攻撃から保護するよう設計されています。OCI WAFは、サイバー攻撃からWebアプリケーションを保護する、レイヤー化された手法を用いたセキュリティ・サービスのスイートを提供します。

このリリースには、事前定義されたOpen Web Access Security Project（OWASP）ルール、アプリケーション固有のルール、およびコンプライアンス・ルールの250を超えるルールが含まれています。OCI WAFは、Webroot BrightCloud®など、複数のソースを集約した、脅威に関するインテリジェント機能も提供します。管理者は、ジオロケーション、IPのホワイトリストとブラックリスト、HTTP URLおよびヘッダーの特性に基づき、独自にアクセス制御を追加できます。ボット管理機能では、JavaScript受け入れ、CAPTCHA、デバイス・フィンガープリンティング、人による相互作用アルゴリズムなど、より高度なチャレンジのセットを提供します。アプリケーションをOCI WAFに登録することで、レイヤー7サービス拒否（DDoS）攻撃から保護します。

OCI WAFの仕組み

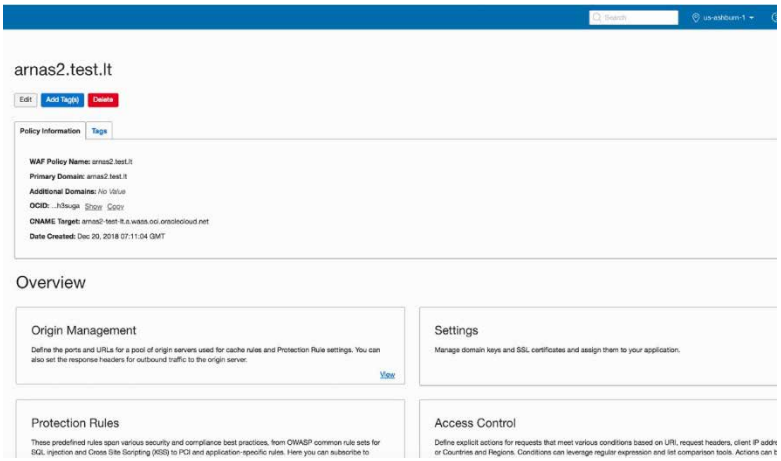
OCI WAFネットワーク・アーキテクチャは、HTTPに対するセキュリティ境界として機能する保護シールドを作成し、WebアプリケーションとAPIの保護における重要なレイヤーを追加します。

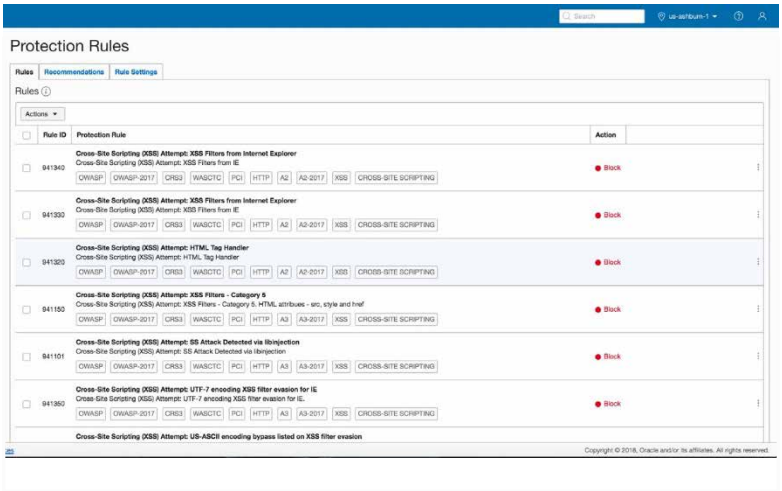
すべてのトラフィックは、アプリケーション・サーバーに到達する前にOCI WAFネットワークを通過します。これにより、OCI WAFはトラフィックを検査し、事前定義されたルールとパラメータに照らし合わせることができます。OCI WAFはリバース・プロキシとして構成されており、Webアプリケーション行きのすべてのトラフィックを検査して、すべての悪意あるトラフィックを識別し、ブロックします。Oracle WAFは、250を超えるルールに基づき、保護対象のWebアプリケーションそれぞれに特化したセキュリティ・プロファイルを提供します。セキュリティ・プロファイルの作成では、トラフィックのプロキシ化によるベースラインの確立、チューニング、およびブロック・モードへの移行が行われます。

主要なOCI WAFコンポーネント

堅牢で効果的なセキュリティ・サービスを提供するための重要な技術的機能として、以下のものが挙げられます。

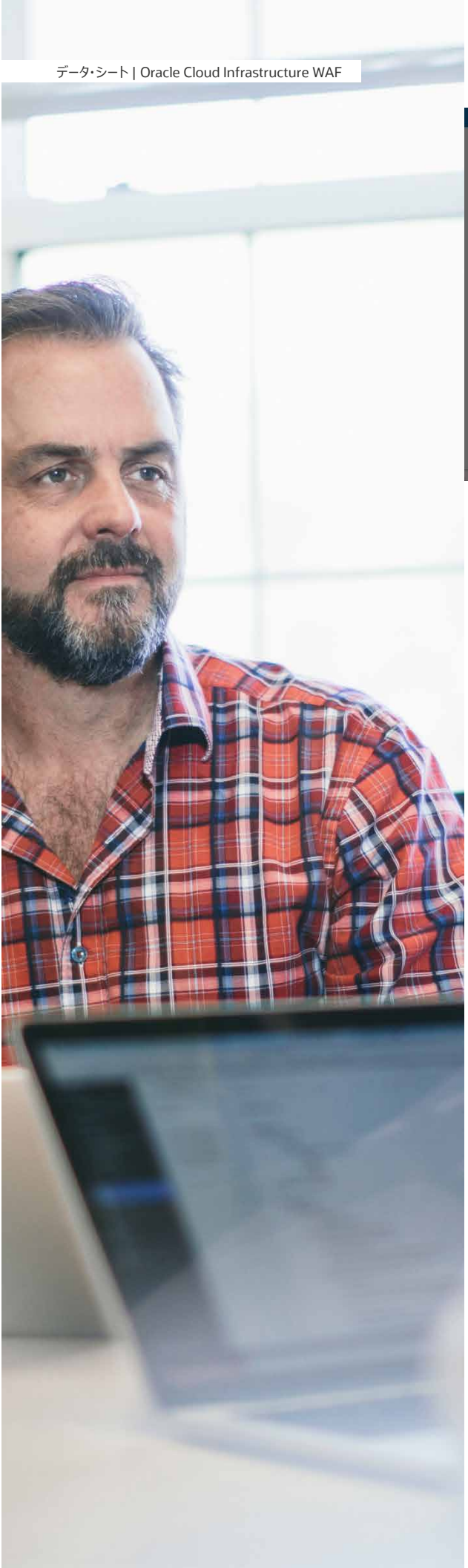
- 厳格な制御および使いやすいOCIセットアップをもたらす、OCIコンソールへの緊密な統合
- SQLインジェクション、クロスサイト・スクリプティング、HTMLインジェクション、およびその他数多くの脅威から保護するOWASPルールセットを含む、250を超えるルールセットをサポート
- JavaScriptチャレンジ、CAPTCHAチャレンジ、ホワイトリスト機能はルールセットと連携。不正なボットをさらに検出、軽減し、人およびボットによる正当なトラフィックを許可
- リスクの高いトラフィック防止のため、ユーザー・アクセス制御は国、IPアドレス、URL、その他のリクエスト属性に基づいて構成可能
- マルチクラウドのサポートにより、インターネットに接続するアプリケーションへのWAFによる保護を提供OCI WAFは、OCI、オンプレミス、ハイブリッド展開、マルチクラウド展開といった環境のワークロードを保護可能
- OCI WAFは各オペレーションについてAPI、SDK、Terraformをサポート。他のOCIサービスとの連携が可能
- 世界各地の研究者と分析能力を備えた、24時間365日対応のセキュリティ運用センター

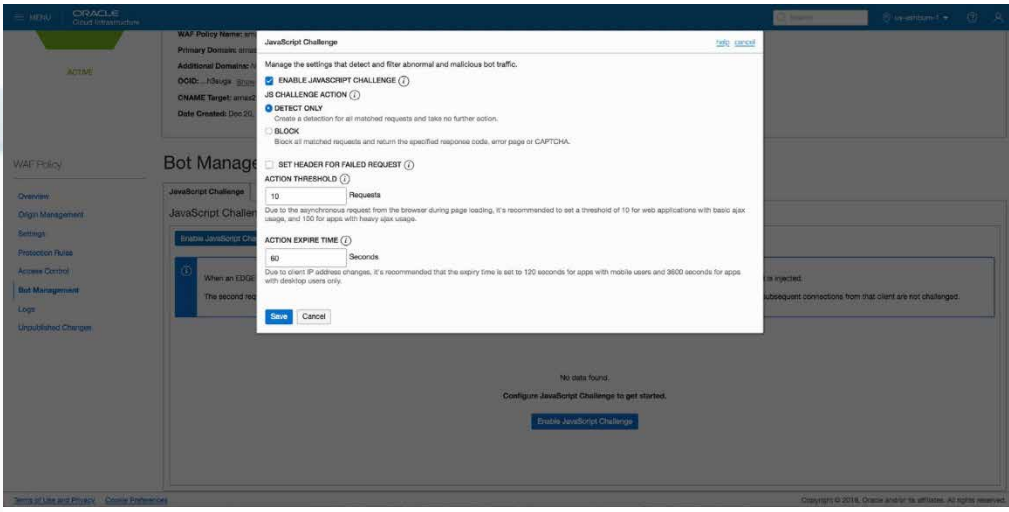




Oracle Cloud Infrastructure コンソールへの緊密な統合

OCI WAFは、WAFポリシーおよびきめ細かなアクセス制御に対する変更の監査など、OCIの他の機能を活用しています。OCI WAFテレメトリは、レポートおよびアラート通知のため、監視サービスに送信されます。コストの追跡および検索のため、コンピューティング、ストレージ、DNSおよびその他のサービスと同様、タグ付けをWAFポリシーに適用できます。





OCI WAFがサポートするルールセットの種類

WAFのルールセットは、サイバー攻撃や悪意のある者から重要なWebアプリケーションを保護します。これらのルールを着信リクエストと照らし合わせて、そのリクエストに攻撃ペイロードが含まれているかどうか判断します。リクエストが攻撃であると判断された場合、WAFはリクエストをブロックするか、またはそのリクエストに関するアラートを送信します。

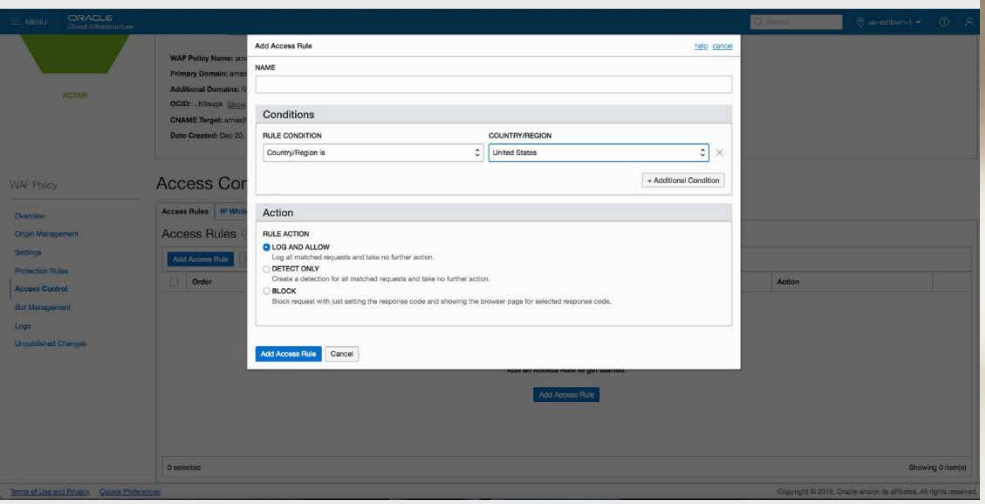
これらの攻撃は、たとえばSQLインジェクション、クロスサイト・スクリプティング、HTMLインジェクションなど、数が多くさまざまですが、OCI WAFルールセットはこれらすべてを検出し、ブロックすることができます。

OWASP 10脆弱性グループの上位は次のとおりです。

- A1 – インジェクション（SQL、LDAP、OSなど）
- A2 – 認証およびセッション管理の不備
- A3 – クロスサイト・スクリプティング（XSS）
- A4 – セキュリティで保護されていない直接オブジェクト参照
- A6 – 機密データ漏洩
- A7 – 機能レベルのアクセス制御不備

OCI Control Centerでは、ルールごとの細かな制御内容とともに、各種類の脆弱性ルールセットが表示されます。

クライアントはそれぞれ独自のルールを作成できます。クライアントでは、登録プロセス時に独自ルールを作成します。OCIでは、すべてのアプリケーション向けの独自ルール、およびWebアプリケーションが必要としたタイミングでの独自ルールのどちらも作成できます。



チャレンジおよびホワイトリスト機能

WAFルールセットとともに、JavaScriptチャレンジ、CAPTCHAチャレンジ、ホワイトリスト機能を追加で使用し、不正なボットをさらに検出、ブロックし、望ましいボットを通過させます。試行失敗回数、有効期限、メッセージなど、チャレンジのパラメータをカスタマイズします。ボットのホワイトリストを使用して、拒否または許可するボットを選択します。

JavaScriptチャレンジ：HTTPリクエストの受信後、すべてのクライアント、攻撃者、実際のユーザーのブラウザにJavaScriptが送信されます。JavaScriptは、ブラウザでアクションの実行を指示します。正当なブラウザは、ユーザーの知識なしでもチャレンジを通過します。ボットは、通常JavaScriptが備わっておらず、チャレンジに失敗し、ブロックされます。これは、ボット攻撃のかなりの割合をブロックできる、迅速で効率的な方法です。

CAPTCHAチャレンジ：ある特定のURLに人間だけがアクセスするようにしたい場合、CAPTCHAによる保護でそのアクセスを制御できます。CAPTCHAチャレンジのコメントは、URLごとにカスタマイズできます。

ホワイトリスト：IPホワイトリストに登録するIPアドレスを自身で管理できます。ホワイトリストに登録されたIPアドレスからのリクエストは、DDoSポリシーやWAFルールセットなど、すべてのチャレンジを通過します。

ユーザー・アクセス制御

アクセス制御を使用して、クリティカルなWebアプリケーション、データ、サービスへのアクセスを制限、制御します。たとえば、地域ベースのアクセスは、GDPRのコンプライアンス要件に適合します。一部のケースでは、特定の国内にとどまることが求められます。地域ベースのアクセス制御は、特定の地理属性を持つユーザーの制限に使用できます。たとえば、アジアの国々との取引が許可されていない場合、それらの国からのアクセスを完全にブロックできます。

- HTTPヘッダー情報に基づきアクセスを制御します。HTTPヘッダーに特定の名前や値が含まれている場合はリクエストをブロックしたり、適切なHTTP正規表現を含むトラフィックは許可したりします。
- URLアドレスの一致か部分一致、または適切なURL正規表現の一致に基づいてアクセスを制御します。

マルチクラウドのサポート

クラウド・プロバイダの多くが、WAFによる保護を自らのクラウド内に存在するアプリケーションに限定しています。これは、OCI WAFには当てはまりません。OCI WAFは、OCIワークロードに対するWAF保護に加え、オンプレミス環境とマルチクラウド環境も保護します。任意の環境のワークロードをOCI WAFだけで保護していることは、OCIに移行する場合に非常に重要です。こうすることで、環境全体に加え、クラウドのテスト、移行、拡張を含む、OCI移行の各フェーズを保護します。

統合のためのAPIサポート

OCI WAFを既存の管理システムやSIEMに直接統合したいと考えているOCIの顧客、パートナー、またはマネージド・サービス・プロバイダであれば、WAFのログをRESTful API経由で取り込むことができます。ログ形式は解析しやすく、リクエスト・メタデータが豊富です。今後のリリースでは、OCIバケットでログ・ファイルを利用できる予定です。

業界をリードする専門知識

オラクルは、世界各地の研究者と分析能力を備えた、24時間365日対応のセキュリティ運用センターを提供します。

ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructureは、企業向けIaaS（infrastructure as a service）プラットフォームです。あらゆる規模の企業が、ミッション・クリティカルなパフォーマンスとコアツーエッジのセキュリティを備えたOracle Cloudでエンタープライズ・アプリケーションおよびクラウドネイティブ・アプリケーションを実行しています。コンピューティング、ストレージ、ネットワーキング、データベース、コンテナを含め、従来のワークロードと新たなワークロードの両方を包括的なクラウドで実行することにより、Oracle Cloud Infrastructureは運用面の効率を著しく向上させ、総所有コストを大幅に減少させることができます。詳しくは、cloud.oracle.com/iaasをご覧ください。