IMPERVA®

ThreatRadar：Web アプリケーション Threat Intelligence

データシート

オンライン事業に影響を及ぼす脅威を事前に防御

サイバー犯罪は、インターネット上の Web アプリケーションの脆弱性につけ込んでこれを最初の攻撃軌道とし、従来のセキュリティ制御をすり抜け、IT インフラストラクチャを移動し、ビジネス・クリティカルなデータおよびアプリケーションにアクセスします。そのような攻撃者の能力は成長し続け、その計略は規模を拡大し、その手法は驚くほど巧妙です。

高度なサイバー攻撃から保護するためには、常に進化している Web ベースの攻撃を防御するための高度な警告システムが不可欠です。このような場合、信頼性の高いクラウドソースのプラットフォームのコミュニティによる Threat Intelligence が非常に重要です。Imperva ThreatRadar は、最高レベルの Threat Intelligence の機能であり、業界最先端[1] の SecureSphere Web Application Firewall（WAF）には以下のような保護機能が実装されています。

- レピュテーション・サービス：最新でリアルタイムのソース・レピュテーションに基づいてトラフィックをフィルタ
- コミュニティ・ディフェンス：Imperva ユーザのクラウドソーシングによる独自の Threat Intelligence を追加
- ボット・プロテクション：ボットネット・クライアントおよびアプリケーション DDoS 攻撃の検出
- アカウント・テイクオーバー・プロテクション：Web サイトのユーザ・アカウントを攻撃や乗っ取りから保護

Imperva ThreatRadar は、業界最先端[1] の SecureSphere Web Application Firewall を実装した最高レベルの Threat Intelligence の機能です。

[1] Gartner社の2015年7月15日付け「Magic Quadrant for Web Application Firewalls」

Imperva ThreatRadarサブスクリプション・サービス

- レピュテーション・サービス
- コミュニティ・ディフェンス
- ボット・プロテクション
- アカウント・テイクオーバー

Threat Intelligence を活用し、悪意あるユーザおよび自動化された攻撃を防御

クラウドソースの Threat Intelligence で新しい攻撃軌道を識別

ThreatRadar は、Imperva アプリケーション・ディフェンス・センタ（ADC）の Threat Intelligence 研究を利用しています。この研究は、データおよびアプリケーションにおける世界屈指の専門家数名によって行われており、これを SecureSphere WAF のお客様のコミュニティからの最新の脅威データと組み合わせて活用しています。

悪意あるソースの早期検出とブロック

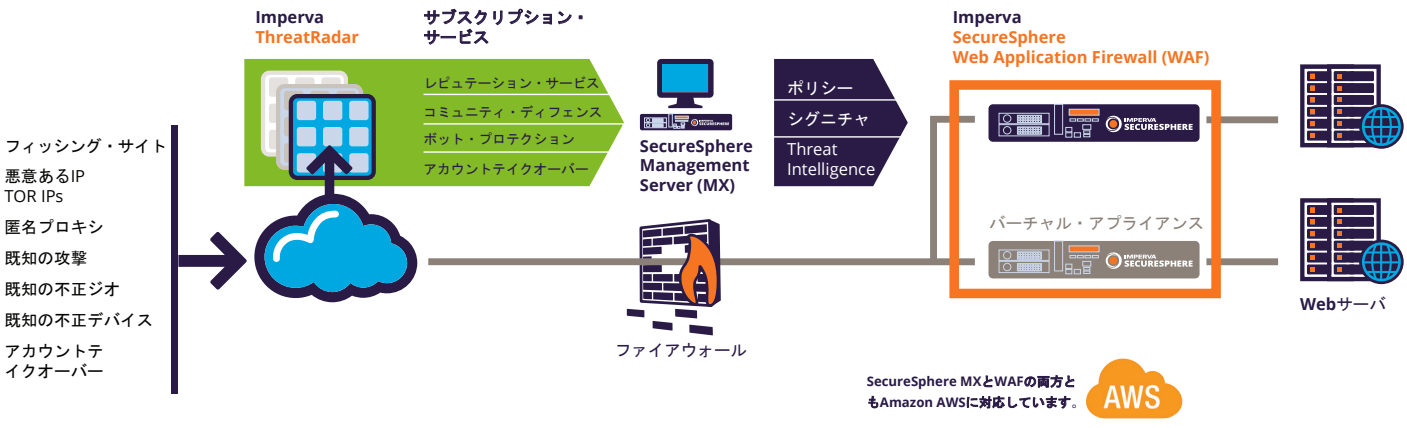
サードパーティのセキュリティ・プロバイダと世界中に導入されている SecureSphere WAF の両方から攻撃データを集約することで、ThreatRadar は既知の悪意あるソースを早期に検出し、包括的に防御します。

脅威データの有効性を向上させて、セキュリティ運用の負荷を軽減

SecureSphere WAF のお客様は、ユーザのレピュテーション、ボットネット、アカウントテイクオーバー、あるいは、ハッカーがアプリケーションの弱点を見つけるために行う調査に基づいて、Web 要求を自動的にアラートまたはブロックすることで、悪意ある、または不要な Web トラフィックに関するセキュリティ運用の負荷を大幅に軽減できます。

最新の攻撃源に関する継続的な自動フィード

ThreatRadar は、ほぼリアルタイムに複数の攻撃フィードを自動配信します。セキュリティ・フィードは、SQL インジェクション、クロスサイト・スクリプティング、DDoS、およびその他の Web 攻撃を、最近実行したソースを特定します。



既知の悪意あるソース

- 攻撃の 90%は既知の悪意あるソースからのもの
- トラフィックの 60%は悪意あるボットからのもの
- Web 攻撃の 50%は盗まれた認証情報の使用によるもの

出典：ImpervaおよびVerizon DBIR

明確な関連アラートとレポートを使用した効率的なフォレンジック分析

ThreatRadar の場合、セキュリティ・イベント分析に推測を用いることはありません。ユーザのレピュテーションや地理的位置データは、追加コンテキストを提供し、正確なインシデント応答を可能にして運用上の負荷を最小限にします。

ThreatRadar Reputation Service

ThreatRadar Reputation Service では、SecureSphere WAF に、次のような悪意ある既知のソースに対処するリアルタイムの Threat Intelligence が実装されます。

- 悪意ある IP アドレス：他の Web サイトを繰り返し攻撃しているソース
- 匿名プロキシ：真の場所を隠すために攻撃者によって使用されているプロキシ・サーバ
- TOR ネットワーク：攻撃源を隠ぺいするために TOR（The Onion Router）を使用しているハッカー
- IP 地理位置情報：攻撃者のアクセスをブロックする地理位置
- フィッシング URL：フィッシング攻撃に使用された不正なサイト（URL）
- コメントスパム実行者：既知のアクティブなコメントスパム実行者の IP アドレス

ThreatRadar Community Defense

ThreatRadar Community Defense は、世界中に導入されている SecureSphere WAF から収集された有益な情報を活用して、各 SecureSphere WAF にほぼリアルタイムにクラウドソースの Threat Intelligence を配信します。特許出願中のアルゴリズムを使用して最新の攻撃データを翻訳し、攻撃パターン、ポリシー、およびレピュテーション・データを収集して、Imperva WAF のお客様が閲覧できるようほぼリアルタイムで Threat Intelligence を配信します。

ThreatRadar Reputation Services が業界をリードする外部のセキュリティ・プロバイダからのセキュリティ情報に依存している一方で、ThreatRadar Community Defense は、世界中に導入されている SecureSphere WAF から収集された最新の攻撃情報を利用しています。

ThreatRadar クラウドへの匿名化攻撃データの送信をオプトインした SecureSphere WAF のお客様は、ThreatRadar Community Defense を無料で受け取ることができます。

ThreatRadar Bot Protection

ThreatRadar Bot Protection サービスを利用すると、SecureSphere WAF で、受信トラフィックを本物のユーザからのものかボット・トラフィックからのものかを正確に判断したり、「良い」ボットか「悪い」ボットかを判断したり、ブラウザの種類ごとにトラフィックを分類したりできます。

悪意あるボットの割合は、DDoS 攻撃、コメントスパムのインジェクション、Web サイト・コンテンツのスクレイピングを含めたすべての Web サイト攻撃の 95%以上を占めます。全 Web サイト・トラフィックの最大 30%をも占める不要なボットを排除すれば、Web サイトのパフォーマンスとセキュリティを改善できます。

Imperva SecureSphere のサイバー・セキュリティ

Imperva SecureSphere は、SecureSphere Web、Database and File Security を含む、包括的で統合されたセキュリティ・プラットフォームです。大企業のデータセンタのセキュリティ要求にも応えられるよう拡張でき、ますます高まる脅威に対して製品の最先端の防衛を行っているワールドクラスのセキュリティ研究機関である Imperva アプリケーション・ディフェンス・センタによって支援されています。

ThreatRadar Account Takeover Protection

犯罪者は、マルウェアやフィッシング攻撃によって認証情報を盗み、顧客のアカウントへの許可されていないアクセスを実行し、お金を送金したり、不正なトランザクションを行ったり、企業の評判を貶めたりします。ThreatRadar Account Takeover Protection を利用すると、SecureSphere WAF で、認証情報／デバイス Threat Intelligence を活用して、そのような許可されていないアクセスを検出および軽減できます。

Credential Intelligence：検出と軽減

- 搾取した認証情報を使用した認証情報スタッフィング
- 脆弱なパスワードを使用した辞書攻撃
- 特権アカウントのデフォルト・パスワード攻撃

Device Intelligence：検出と軽減

- リスクの高いデバイスからのデバイス・ログイン
- TOR ／プロキシに隠れたデバイスからのトランザクション
- ジオベースのリスクの高い場所—ISP、ジオ／ IP の不一致
- 単一のアカウントにアクセスする複数のデバイス、短時間に複数のアカウントにアクセスする単一のデバイス

ThreatRadar のエディション

ThreatRadar には、ご購入しやすく、実装コストを削減していただけるよう、次の 2 つのバンドルに Reputation Services、Community Defense、Botnet Protection の 3 つのサブスクリプション・フィードが含まれています。

ThreatRadar Community Edition

クラウド上の Imperva グローバル ThreatRadar リポジトリを使用して、お客様の SecureSphere WAF から最新の攻撃データを共有することをオプトインしたお客様がこのバンドルを使用できます。お客様固有のデータはすべて自動的に匿名化されます。

ThreatRadar Enterprise Edition

クラウド上の Imperva ThreatRadar リポジトリを使用して、お客様の SecureSphere WAF から最新の攻撃データを共有することをオプトアウトしたお客様がこのバンドルを使用できます。これらのお客様は、世界中に導入されている SecureSphere WAF から収集された有益な情報を取得でき、また、Imperva ADC の最高レベルの脅威研究の恩恵を受けることができます。

DS-SECURESPHERE-THREATRADAR-A4-1015-rev2