imperva

機能紹介

Runtime Application Self-Protection (RASP)

デフォルトでアプリケーションを保護する

アプリケーションは、個人情報、知的財産、財務情報、その他重要なデータを扱うため、サイバー攻撃の恰好のターゲットとなります。従来のアプリケーションセキュリティツールでは、シグネチャやルールに依存するため、パフォーマンスの低下を招き、誤検知やゼロデイ攻撃に悩まされています。また、リアルタイムでのコンテキストや可視性がなく、企業を攻撃から守ることができません。Imperva が考えるアプリケーションの保護とは、アプリケーションが自ら攻撃から守るという根本的な考えによるものです。

Imperva RASP

Imperva RASP は、レガシーアプリケーションと最新のアプリケーションを両方保護するプラグインで、アプリケーションのセキュリティのギャップを埋めるものです。RASP プラグインは、オンプレミス、クラウド、コンテナなど、どのようなアーキテクチャでも動作します。Imperva RASP は、言語理論セキュリティ（LANGSEC）と呼ばれる、業界をリードする高速な攻撃検知で、アプリケーションを保護することができます。LANGSEC は、決められた環境のコンテキスト内でペイロードがどのように実行されるか理解し、既知の攻撃やゼロデイ攻撃を阻止します。そのため、アプリケーションソフトウェアにある潜在的な脆弱性に関係なく、導入当初からアプリケーションの安全性を確保できます。

RASP は、アプリケーション開発のライフサイクルにセキュリティを統合し、アプリケーションセキュリティに対する従来の脆弱性管理を補強します。RASP は、ブロックされた攻撃が利用したと思われる脆弱性を、コード行まで特定し、脆弱性があってもアプリケーションを保護します。これにより、脆弱性のパッチは、企業側のスケジュール及び都合に応じて適用できます。

主な機能:

- オンプレミス、クラウド、コンテナなど、場所を問わずアプリケーションを保護
- シグネチャ、学習モード不要で、価値創出の時間短縮
- 既存のビルドパイプラインを使用し、ネットワークの呼び出し無しのシンプルな導入
- オリジナル、サードパーティソフトウェアの潜在的な脆弱性を保護
- ゼロデイ攻撃からの保護
- すぐに使えるレポート機能

FORRESTER®
NEW WAVE LEADER 2018
Runtime Application Self-Protection

Forrester 社の調査レポートによると、Imperva の RASP（旧称 Prevoty（これは、製品名称が Prevoty から変わったわけではなく、Prevoty 社を Imperva が買収したということです））が業界をリードしていることが明らかになりました。

The Forrester New Wave™: Runtime Application Self-Protection 2018年第1四半期。Forrester社のレポート全文はこちらからダウンロードできます。

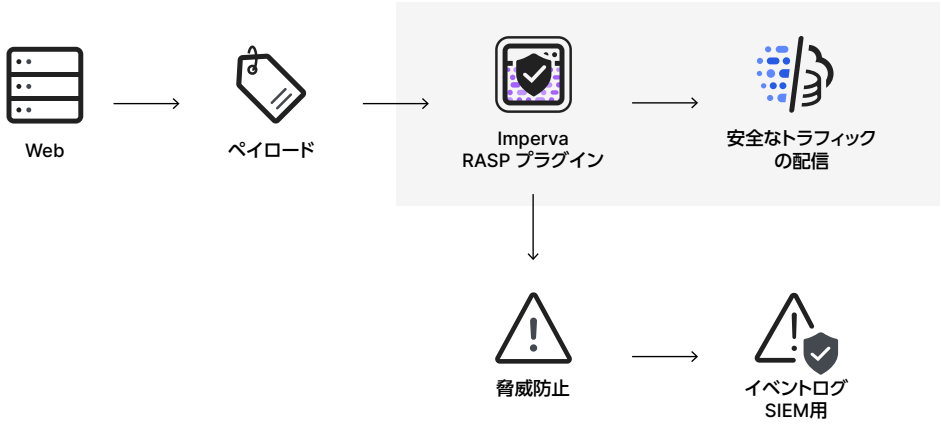

図 1： Imperva RASP プラグインはアプリケーション内部に配置され、リアルタイムで完全なアプリケーションコンテキストで脅威を解析し、脅威をブロックしながら信頼できるサイトのトラフィックを提供します。

Imperva RASPの概要

Imperva Runtime Application Self-Protectionのメリット

- RASP で保護された稼働中のアプリケーションは、場所や用途に関わらずデフォルトで安全です。
- RASP にはシグネチャの更新、学習モードは不要で、外部ネットワークからの呼び出しも必要なく、特許取得済みの LANGSEC 技術で、CPU やメモリの消費もほとんどありません。そのため、低コスト（TCO）ですぐに実現できます。
- RASP は、オリジナルソフトウェア、サードパーティのソフトウェアに関係なく、アプリケーションの安全性を確保し、脆弱性の修正とパッチの適用の時間を確保できます。
- RASP は、アプリケーション攻撃、イベントそしてリスクを、アプリケーション内部から可視化でき、セキュリティコンテキストを強化します。

DevOpsに合わせて拡張可能な導入

RASP は、アプリケーションの内部で自律的に動作するプラグインによって、速やかに導入されるため、導入場所や方法を選びません。RASP は、高い検出精度と非常に低いパフォーマンスオーバーヘッドを併せ持つ LANGSEC 技術を利用しているため、導入の影響が少なく、重要なビジネス機能はユーザーエクスペリエンスを損なうことなく継続することができます。

Imperva RASPは、次のアプリケーションをサポートしています:

- コマンドインジェクション
- クリックジャッキング
- クロスサイトスクリプティング(XSS)
- クロスサイトリクエストフォージェリ(CSRF/XSRF)
- データベースアクセス侵害(Advanced SQLi)
- HTMLインジェクション
- HTTPメソッド改ざん
- HTTPレスポンス分割
- セキュリティで保護されていないCookie
- セキュリティで保護されていないトランスポート
- JSONインジェクション
- ラージリクエスト
- 機密情報のログ収集
- 不正なContent-Types
- OGNLインジェクション
- ディレクトリトラバーサル
- SQLインジェクション
- 機密情報のログ収集
- セキュリティで保護されていないトランスポートプロトコル
- 不正なネットワーク操作
- 未捕捉例外
- 無効なリクエスト
- 脆弱な依存関係
- 脆弱な認証
- 脆弱なブラウザのキャッシュ管理
- 脆弱な暗号化と暗号
- XML 外部エンティティ インジェクション(XXE)
- XMLインジェクション
- その他

Imperva Application Security

RASP は Imperva アプリケーションセキュリティの重要な要素の 1 つで、最適なカスタマーエクスペリエンスを提供しながらリスクを低減します。オンプレミスおよびクラウド上のアプリケーションを以下の方法で保護します:

実用的なセキュリティインサイトを提供

DDoS 攻撃からの保護

ボット攻撃の緩和

すべてのデータの流れを監視

WAF の機能による保護

API を標的とするサイバー攻撃からの保護

最適なコンテンツ配信の実現

Imperva Application Security についての詳細は、imperva.com/ja までお問い合わせください。

Imperva は、データやアプリケーションの安全性を追求する、アナリストに認められたサイバーセキュリティのリーダーです。

imperva.com
+1.866.926.4678