IMPERVA®

Imperva Incapsula Webサイト・セキュリティ

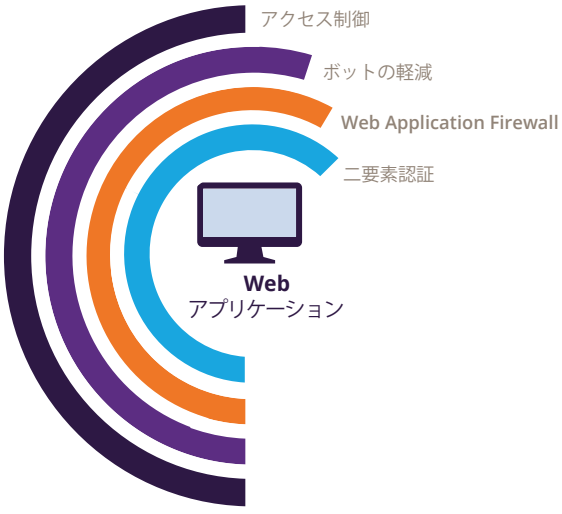
データシート

クラウドを利用したアプリケーション・セキュリティ

クラウドベースのWebサイト・セキュリティ・ソリューションであるImperva Incapsulaは、業界をリードするWAF技術に加え、強力な二要素認証およびボット・アクセス制御を特長とします。高度なクライアント分類エンジンにより、サイトが受信するすべてのトラフィックを分析し、悪意のある不要な訪問者のアクセスを防止します。また、WAFの組み込みセキュリティ機能を補完し、企業が独自の要件に合わせたカスタム・セキュリティ・ルールを容易に構築できるツールを提供します。

お客様のメリット

- クラス最高のPCI認定 Web Application Firewall
- 企業のセキュリティ・ポリシーおよび使用事例に合わせたカスタム・ルール
- Webサイト・アクセスのための二要素認証
- すべての受信トラフィックを分析する高度なクライアント分類エンジン
- バックエンド・システムと統合するための使いやすいAPI



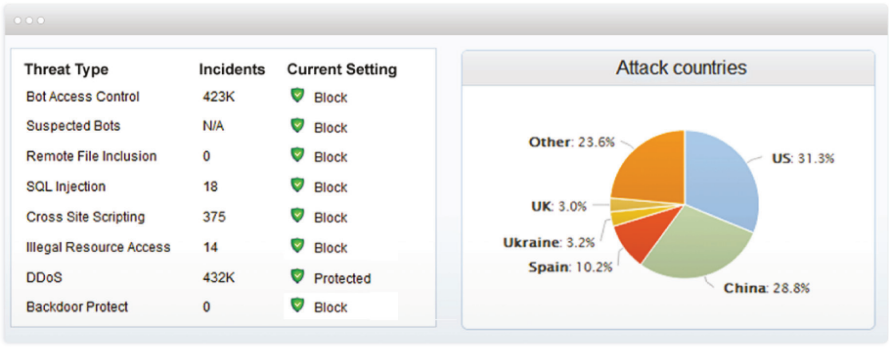
Incapsulaを選択する理由

- 顧客ベースを活用したクラウドベースのビッグ・データ・アプローチにより、攻撃状況を360度可視化
- 毎日実行される何百もの侵入テストおよび何百万もの攻撃に対して実証済み
- 専任のセキュリティ調査チームがサービスを監視、調整、更新し、新たに出現した脅威から確実に防御
- 何十年にもわたるセキュリティに関する経験とベスト・プラクティスを持ち、Impervaの市場をリードするWAF技術を活用
- 簡単なDNS変更のみでアクティベート可能で、ハードウェアやソフトウェアのインストール、統合、またはWebサイトの変更が不要

クラウドベースのビッグ・データ・セキュリティ・アプローチ

クラウドベースのアプローチにより、顧客ベースから得た実データを利用することでグローバルな攻撃状況をより深く理解し、セキュリティを継続的に向上させます。サンドボックス機能により、実際のWebサイト上で新機能のリリース前に非公開でテストすることもできます。Incapsulaは、何千ものお客様にサービスを提供し、日々何百もの侵入テストや何百万もの攻撃に対処し、最も厳しいセキュリティ基準を満たすよう調整されています。

Incapsulaはクラウドソーシング技術を利用し、現在の脅威の状況について蓄積された知識に基づいてWebサイトを保護します。脅威情報は、ビッグ・データ分析を使用し、Incapsulaコミュニティ全体から収集されます。このデータは、新たに発生した攻撃を識別し、Incapsulaの保護対象となるすべてのWebサイトに被害軽減化ルールを適用するために使用されます。



Web Application Firewall (WAF)

業界をリードするWAF技術

Incapsulaは、Webサイトとアプリケーションを常にあらゆるタイプのアプリケーション・レイヤーのハッキングの試みから確実に保護するクラウドベースのWAFを提供します。Impervaの業界をリードするWAF技術と経験に基づき、当社のWAFはOWASP Top 10の脅威から保護します。これには、SQLインジェクション、クロスサイト・スクリプティング、不正なリソースへのアクセス、リモート・ファイル・インクルージョンが含まれます。Incapsulaを支えるセキュリティ専門家により、新しく発見された脆弱性からも最適に保護し、アプリケーションの中断を防止し、Webサイトのパフォーマンスを向上させます。

積極的な修復

Incapsulaのセキュリティ・チームは、ハッカーの活動やゼロデイ攻撃を監視し、当社のサービスを使用するWebサイトやアプリケーションを確実に保護します。Incapsulaは、すべての一般的なWebサイトのスタックやコンテンツ管理システム、eコマース・ソリューションに対し専用データベースを使用し、専用セキュリティ・ルールを適用して、これらのソースからの既知の脆弱性を積極的に修復します。新しく発見された脆弱性に対しても保護を提供し、アプリケーションの中断を防止し、Webサイトのパフォーマンスを向上させます。

PCI認定とレポート作成

当社のWAFは、PCI Security Standards Councilにより認定されています。これにより、お客様の機密データがサイト上で漏洩するのを防ぐとともに、お客様を責任や違反に対する罰金からも保護します。Incapsula PCIコンプライアンス・レポートはセキュリティ・ルールの設定変更を監査し、PCI要件6. 6への準拠を定期的に報告します。豊富なグラフィカル・レポート作成機能により、企業は容易にセキュリティ状況を把握し、法規制コンプライアンスを満たすことができます。

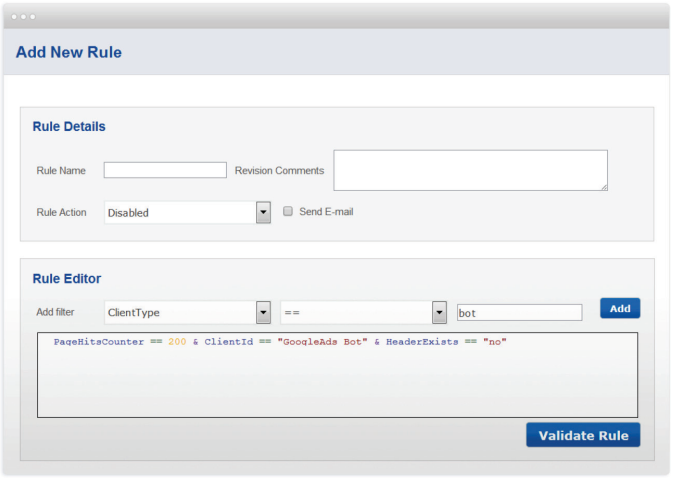
ブラックリストへの掲載防止

アプリケーションの脆弱性のために、毎日、多くの正当なWebサイトがセキュリティ・ソフトウェアRMS、検索エンジン、およびブラウザ・ベンダのマルウェア・ブラックリストに追加されています。このような場合、お客様やパートナーはWebサイトへのアクセスができず、ビジネスが事実上中断してしまいます。WAFはアプリケーションの脆弱性のギャップをなくし、ブラックリストへの掲載を回避し、Webサイトへのアクセスが常時可能な状態を実現します。

カスタム・セキュリティ・ルール

カスタム・セキュリティ・ルールにより、各企業は最適な方法で、IncapsulaのWebサイト・セキュリティ・サービス内に独自のセキュリティ・ポリシーを適用することができます。使いやすいGUIにより、組織固有のニーズを満たすカスタム・セキュリティ・ルールを設定できます。

カスタム・セキュリティ・ルールは、機密領域のセキュリティ・ポリシーを強化する、または調査が必要な特定のイベントに対するアラートを生成するなどの機能を提供し、クラス最高のWebアプリケーションのセキュリティ機能を強化します。これらのルールはセキュリティを向上させるだけでなく、特定のユーザ挙動の特異性を考慮し、誤検出をなくします。



技術に関する知識の有無にかかわらず、ユーザは直感的なGUIルール・ビルダまたは構文テキスト・エディタを用いて、カスタム・ルールを定義できます。ルール・アクションには、アラートやブロック・リクエスト、ブロックIP、またはリクエストCAPTCHAを含めることができます。また、ルール・トリガはURLやクライアント・タイプ、ユーザ・エージェントなど複数の項目に基づきます。

カスタム・ルール・トリガの例：

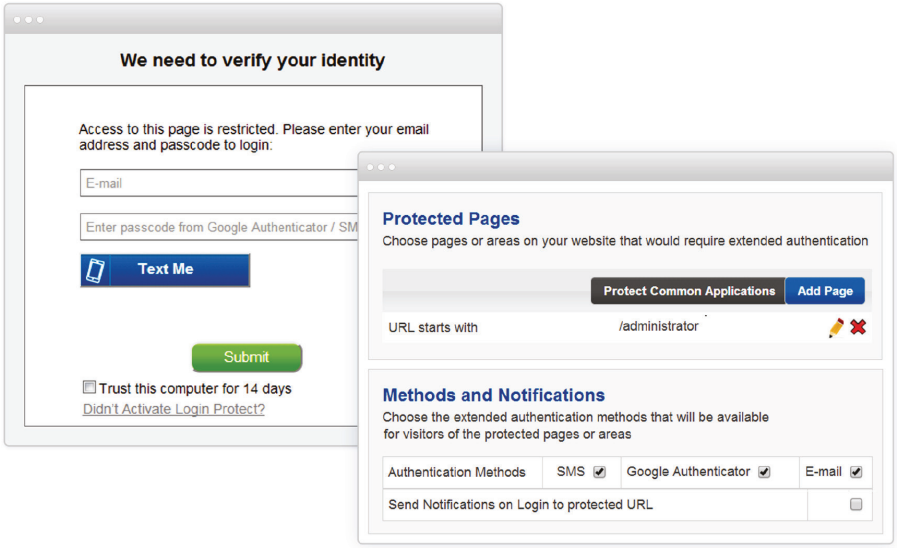
- (ClientType == Browser | Referrer contains google.com)
- (User-Agent contains googlebot & CaptchaState == Failed | ClientIP == 120.0.0.1).

ボットの軽減

すべてのWebサイト攻撃の95%以上が悪意のあるボットによって行われています。Incapsulaは、高度なクライアント分類技術やクラウドソーシング技術、レピュテー ションに基づく技術を使用し、「正当」なボット・トラフィックと「不正」なボット・トラフィックを識別します。これにより、GoogleやFacebook、Pingdomなどの正当なボットが自由にWebサイトにアクセスできるようにしながら、迷惑コメントやスクレイピング、脆弱性スキャンなどの既知の不正なボットや疑わしいボットの行動をブロックできます。悪意のあるボットは全Webサイト・トラフィックの最大50%を占めるため、悪意のあるボットをブロックすることにより、セキュリティの向上に加え、Webサイトのパフォーマンスも向上します。

二要素認証

Incapsulaにより、統合やコーディング、ソフトウェアの変更なしに、あらゆるWebサイトやアプリケーションに強力な二要素認証を実装できます。クリック1つでアクティベーションされ、即座に管理アクセスを保護し、企業のWebアプリケーションへのリモート・アクセスを保護し、特定のWebページへのアクセスを制限することができます。二要素認証は、いくつかのWebサイトにまたがる複数のログインを一元的に管理、制御します。また、電子メール、SMS、またはGoogle認証のいずれかを使用してサポートされます。



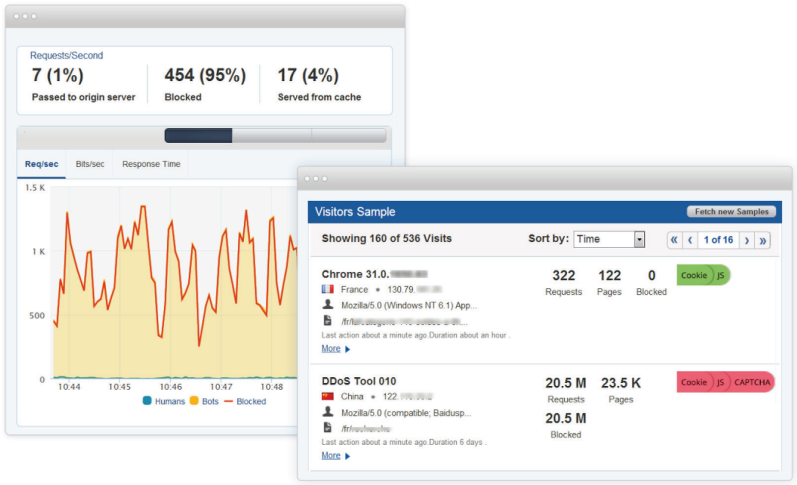
トラフィック監視と分析

詳細な脅威レポートと分析

アラート通知は容易に検索、ソートすることができ、対応するセキュリティ・ルールに直接リンクされています。Incapsulaの監視およびレポート作成フレームワークは、セキュリティ、コンプライアンス、コンテンツ配信に関連する懸念を速やかに可視化します。ダッシュボードは、システム状況およびセキュリティ・イベントの高レベル・ビューを提供します。Incapsulaは、Webサイトにもたらされるあらゆる脅威の詳細な分析をお客様に提供します。これには、IPアドレス、ユーザ・エージェント、場所、およびその他の関連セッション情報が含まれます。週次のグラフィカル・レポートは、Webサイトのトラフィック、脅威、およびパフォーマンスの向上のトレンドを可視化します。

リアルタイム統計

リアルタイム統計ダッシュボードにより、ユーザはWebサイトのトラフィックとパフォーマンスに関する生の情報に瞬時にアクセスできます。このプレミアムな機能により、セキュリティ・イベントへの迅速な対応と、リアルタイムのデータ駆動型の意思決定が可能となります。例えばDDoS攻撃の場合、生のトラフィック統計により、セキュリティ・チームが即座にボットや訪問者の異常な行動パターンを識別できます。またチームは、サーバが攻撃の負荷にどれだけ適切に対処しているかを評価し、そのデータを使用してサーバ間の負荷分散を最適化することができます。



プレミアムなサービス・サポート

マネージドサービス

Incapsulaは、組織が他のビジネス・クリティカルなタスクのためにITリソースを解放できるよう、マネージドサービス・オプションを提供します。当社のマネージドサービスは、セキュリティ専門家とサポート・エンジニアの専任チームに基づき、24時間体制で最高レベルのセキュリティとパフォーマンスを実現します。Incapsulaは、継続的なWebサイトの健全性監視に加え、電子メールの脅威アラート、積極的なセキュリティ・イベントの管理、ポリシー・チューニングと設定管理、週次レポートを組織に提供します。24時間年中無休のNOCは継続的なセキュリティ監視を行い、常にDDoS攻撃およびその他の新しく出現した脅威から防御します。マネージドサービスのお客様には個別のアカウント・マネージャが割り当てられ、1つの窓口であらゆるWebサイトのセキュリティやパフォーマンスのニーズに関して問い合わせることができます。

IMPERVA INCAPSULA

プロビジョニング、管理、イベント用API

当社の製品の専門家はエンタープライズWebアプリケーションの世界を理解しており、ITチームと密接に連携し、具体的な統合やカスタマイズの要件に対応します。Incapsula APIはバックエンド・システムと容易に統合できるよう設計され、合理化されたお客様のプロビジョニングとアカウント管理を可能にします。

プラグ&プレイSIEM統合

Incapsulaは、既存のソリューションおよびワークフローを強化するため、HP ArcSightやSplunk、McAfeeなどの主要SIEMプラットフォームとシームレスに統合するコネクタを開発しました。これはネットワーク上に存在し、SIEMとIncapsula API間のリンクとして機能します。SIEMの統合により、ほぼリアルタイムのイベント・レポート作成と強力なデータ暗号化に加え、あらかじめ用意されたカスタム・ダッシュボードとレポートを利用し、セキュリティのベスト・プラクティスに従ってSIEM内からの受信データを容易に確認することができます。