AKAMAI 製品概要

Client-Side Protection & Compliance

クライアントサイドの JavaScript の脆弱性を保護し、規制遵守のプロセスを合理化します

JavaScript は、今や Web アプリケーションにとって不可欠なツールです。ユーザー体験の最適化から、機能とパフォーマンスの強化に至るまで、ファーストパーティーとサードパーティーのいずれにおいても、JavaScript の使用は飛躍的に拡大しています。これにより、さまざまなメリットがもたらされる一方、JavaScript のデジタルサプライチェーンにおいて、Web サイトがクライアントサイドへの攻撃に対して脆弱になる可能性があります。たとえば、悪性のコードをインジェクトして、ペイメントカードのデータなど、エンドユーザーの機微な情報をブラウザー内から盗もうとする攻撃が発生しています。

このような攻撃はサーバーサイドで把握されず、従来のセキュリティ対策を迂回するため、多くの組織が被害を受けてしまいます。そうなれば、顧客の信頼を失い、規制違反による罰金やコンプライアンス違反の対象となり、ブランドの評判が損なわれます。

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance は、エンドユーザーデータの窃取を防ぎ、JavaScript の脅威から Web サイトを守ります。悪性スクリプトのふるまいを検知して、実効性のあるアラートをセキュリティチームに提供することにより、有害なアクティビティをリアルタイムで緩和できるように設計されています。

Client-Side Protection & Compliance には、PCI DSS v4.0 へのコンプライアンスに特化した機能もあるので、新たなスクリプトセキュリティ要件への対応や、クライアントサイドへの攻撃に対するペイメント・カード・データの保護にも役立ちます。決済ページのスクリプトのインベントリを簡単に管理できるだけでなく、包括的な 1 つのダッシュボードで監査プロセスを合理化できます。また、PCI 専用のアラートを受信することで、コンプライアンスに関わるイベントに迅速に対応できます。

主な機能

クライアントサイドでの機微なデータの窃取に対する防御

サイバー犯罪者は、エンドユーザーの機微な情報を狙っています。攻撃者は JavaScript サプライチェーンの脆弱性を悪用することで、Web サイトにコードをインジェクトし、不正な目的のために機微な情報を盗み取ることができます。Client-Side Protection & Compliance は、機械学習とヒューリスティックスコアリングを組み合わせて、スクリプトのふるまいをリアルタイムで分析し、悪性のアクティビティや脆弱なリソースを検知します。また、Web スキミング、Magecart、フォームジャッキングなど、クライアントサイドへの攻撃に対して、実効性のあるアラートを即座にセキュリティチームに送信し、すばやい防御を可能にします。

ビジネス上のメリット

検知と保護：
実際のユーザーセッションにおけるスクリプトのふるまいを監視し、疑わしいアクティビティを検知できます。

PCI DSS v4.0 ワークフロー：
JavaScript セキュリティ要件 6.4.3 および 11.6.1 に対応できます。

優先順位に基づくリアルタイムアラート：
実効性のあるアラートにより、高リスクのイベントを即座に緩和できます。

クライアントサイドへの可視性：
クライアントサイドのアタックサーフェスを広範囲に把握できます。

ポリシー管理：
スクリプトのふるまいを管理し、ランタイム JavaScript 実行を制御できます。

脆弱性の検知：
Akamai 脅威インテリジェンスを活用し、共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）の脆弱性を特定できます。

柔軟な導入オプション：
Akamai Connected Cloud を使用することも、またオリジンサーバーに直接導入することもできます。いずれの方法でも簡単に導入できます

PCI DSS v4.0 コンプライアンスに特化したサポート

PCI DSS v4.0 のスクリプトセキュリティ要件 6.4.3 および 11.6.1 は、クライアントサイドへの攻撃に対してペイメントカードのデータを保護し、決済ページのスクリプトを確実に管理することを義務付けています。Client-Side Protection & Compliance は、決済ページのすべてのスクリプトの追跡とインベントリを実行し、それらの整合性と認可を確保します。正当とみなす基準を事前定義し、ルールを自動化することで、読み込まれるスクリプトすべての正当性を簡単に確認できます。このソリューションには、HTTP ヘッダーや決済ページの保護状態に対する変化を監視する機能もあり、ページの改ざんも防ぐことができます。また、包括的なダッシュボードと、PCI に特化したアラートにより、コンプライアンスに関わるイベントにすばやく対応できるため、ブラウザー内のペイメント・カード・データを確実に保護できます。これらの機能を活用することで、組織内のセキュリティチームやコンプライアンスチームは、PCI 監査プロセスの負担を軽減し、ワークフローの効率化に迅速に取り組むことができます。

JavaScript の脅威に対する広範な可視性

Web アプリケーションファイアウォールを始めとする従来型の Web アプリケーション保護では、監視対象はサーバーサイドのトラフィックのみであるため、クライアントサイドで実行されるアクティビティは把握できません。また、コンテンツ・セキュリティ・ポリシーなど、JavaScript の脅威に対する標準ベースの保護対策も、Web ページのオペレーターの制御が及ばないスクリプトサプライチェーン内に悪性のペイロードが導入された場合は、それらを管理することは難しく、限定的な保護しか提供できません。そのため、このような悪性コードは盲点になりやすく、何日も、何週間も、あるいは何か月にもわたって検知されることなく、機微なデータの窃取を続けることもあります。Client-Side Protection & Compliance は、Web サイトのクライアントサイドのアタックサーフェス、たとえば、各スクリプトのふるまい、脆弱性、到達範囲、影響、アクセスされて脅威にさらされているデータなどに関して、比類のない可視性を提供します。

仕組み

Client-Side Protection & Compliance は、エンドユーザーのブラウザーで稼働し、クライアントサイドのスクリプトが保護対象の Web ページでどのように実行されているかを監視します。スクリプトのふるまいに変化があると、機械学習のテクニックを使用して、不正なまたは不適切なアクションのリスクを評価します。リスクの高いイベントであれば、セキュリティチームに警告するので、潜在的な脅威をすばやく調査して緩和できます。

セットアップ：パフォーマンスに有意な影響を及ぼすことのないシンプルなスクリプトを、監視対象の各ページにインジェクトします。

監視と評価：ユーザーの Web ブラウザーから JavaScript のアクティビティデータを収集し監視します。不正な、または不適切なアクションが見つかると、機械学習のテクニックを使用して、それらのリスクを評価します。

アラート：実際に脅威や攻撃が検知された場合は、リアルタイムのアラートとともに脅威緩和に役立つ詳細情報を送信します。

緩和：悪性の JavaScript に対しては、保護対象の Web ページの機微なデータにアクセスしたり、それらを盗み取ったりできないように、ワンクリックで簡単かつすばやく制限できます。

PCI DSS v4 のスクリプトセキュリティ要件に迅速に対応

スクリプトの整合性と認可（6.4.3）

保護対象の決済ページに読み込まれるすべてのスクリプトの整合性と認可を確保します。

スクリプトのインベントリと正当性確認（6.4.3）

保護対象の決済ページに読み込まれるスクリプトを追跡し、インベントリを作成します。正当とみなす基準を事前定義し、ルールを自動化することで、すべてのスクリプトの正当性を迅速に確認します。

決済ページの保護（11.6.1）

保護対象の決済ページに、認可されていない変更が生じた場合は、即座に検知し対応します。

直感的なダッシュボード

PCI DSS v4.0 のスクリプトセキュリティ要件 6.4.3 および 11.6.1 に関連するタスクとアラートについては、専用のダッシュボードで詳細情報を確認できるため、遵守と監査のプロセスがシンプルになります。

実効性のある PCI アラート

不正なスクリプト、決済データの窃取、決済ページの改ざんなど、PCI コンプライアンスに関わるイベントについては、詳細なアラートが送信され、ログに記録されます。

詳細については、製品ページ、またはAkamai の営業担当チームにお問い合わせください。