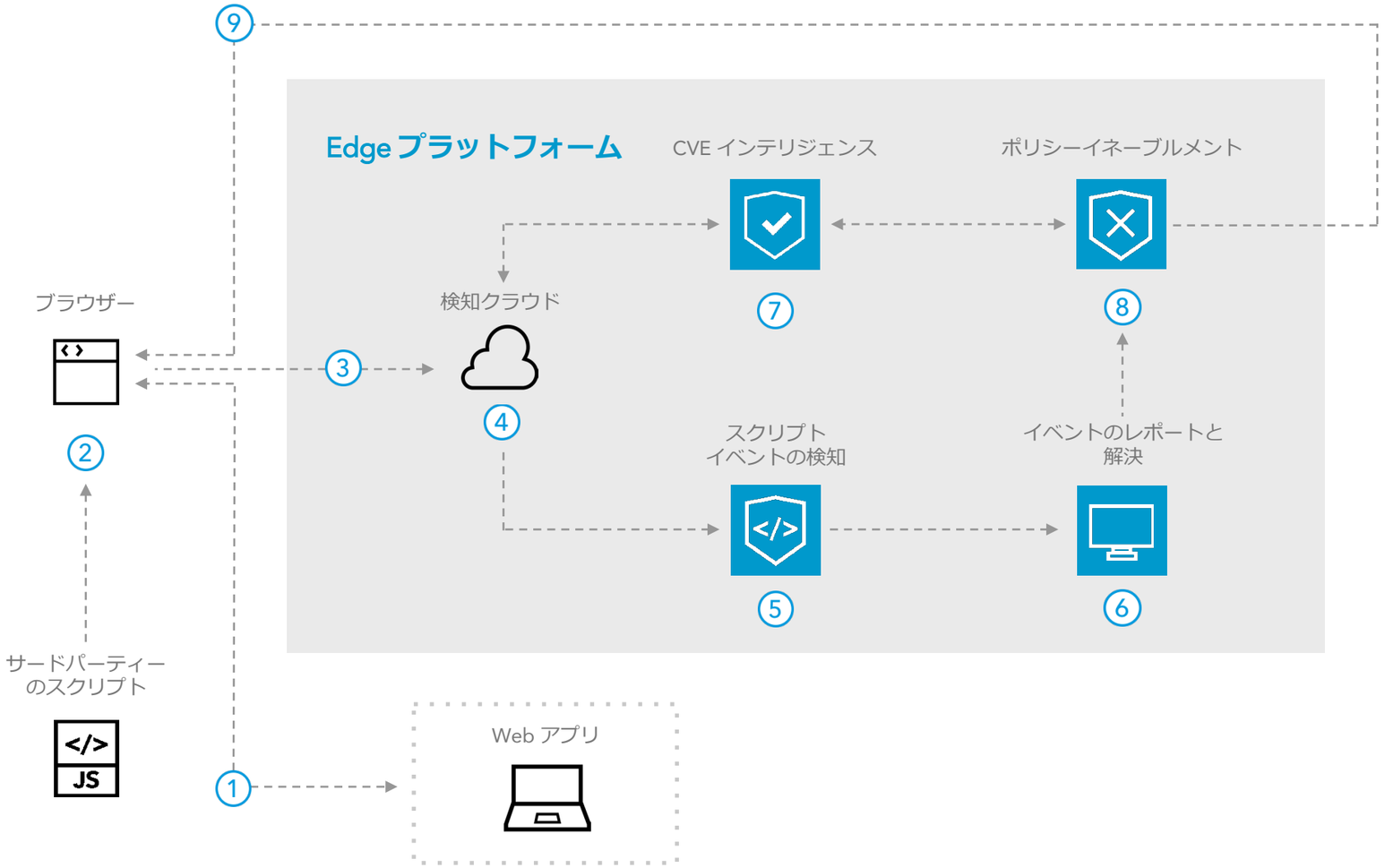
Client-Side Protection & Compliance

リファレンスアーキテクチャ



概要

Client-Side Protection & Compliance が提供する、ふるまいベースのアプローチによるスクリプト保護は、悪性のスクリプトアクティビティを検知して Web ページの整合性を保護し、貴社のビジネスを守ります。

1. ユーザーは、一般的なブラウザーを使用して、Web アプリで生成された HTML ページの機能にアクセスします。一般的なサイトには、平均 100 以上のスクリプトが含まれています。
2. 通常、これらのスクリプトの半数以上は、サードパーティーのパートナー（サードパーティーのスクリプト）から直接リクエストされ、サードパーティーのパートナー（サードパーティーのスクリプト）に直接配信されます。
3. ブラウザー内でスクリプトが実行されると、Akamai は実行情報を検知クラウドに送信します。そして、スクリプトのふるまいに異常がないかどうかを調べます。
4. 疑わしい異常が見つかった場合は、リアルタイムで分析し、機微な情報へのアクセスや宛先サーバーの指定に関するスクリプトのふるまいの変化に注目しながら、リスク要因の数に基づいてリスクスコアを割り当てます。
5. 疑わしい異常については、必要に応じて、強調表示し、概要としてまとめて、記録し、アラートを送信します。
6. セキュリティチームはイベントの重大度を示すアラートと詳細情報を受信します。疑わしい異常が悪性だった場合は、イベントを直ちにブロックし、ポリシーを作成できます。
7. 異常検知と並行して、収集したスクリプトデータを Akamai Common Vulnerabilities and Exposures（CVE）のインテリジェンスと比較照合し、セキュリティ上のギャップと脆弱性を特定します。
8. 発見されたCVE の弱点を Client-Side Protection & Compliance のポリシーに追加することで、機微なデータの流出を継続的にブロックできます。
9. スクリプト防御機能が検知した脅威に基づき、発信ポリシーを通じて機微な情報の流出を防御できます。

キープロダクト

スクリプト保護 ► Client-Side Protection & Compliance

公開日：2023 年 10 月