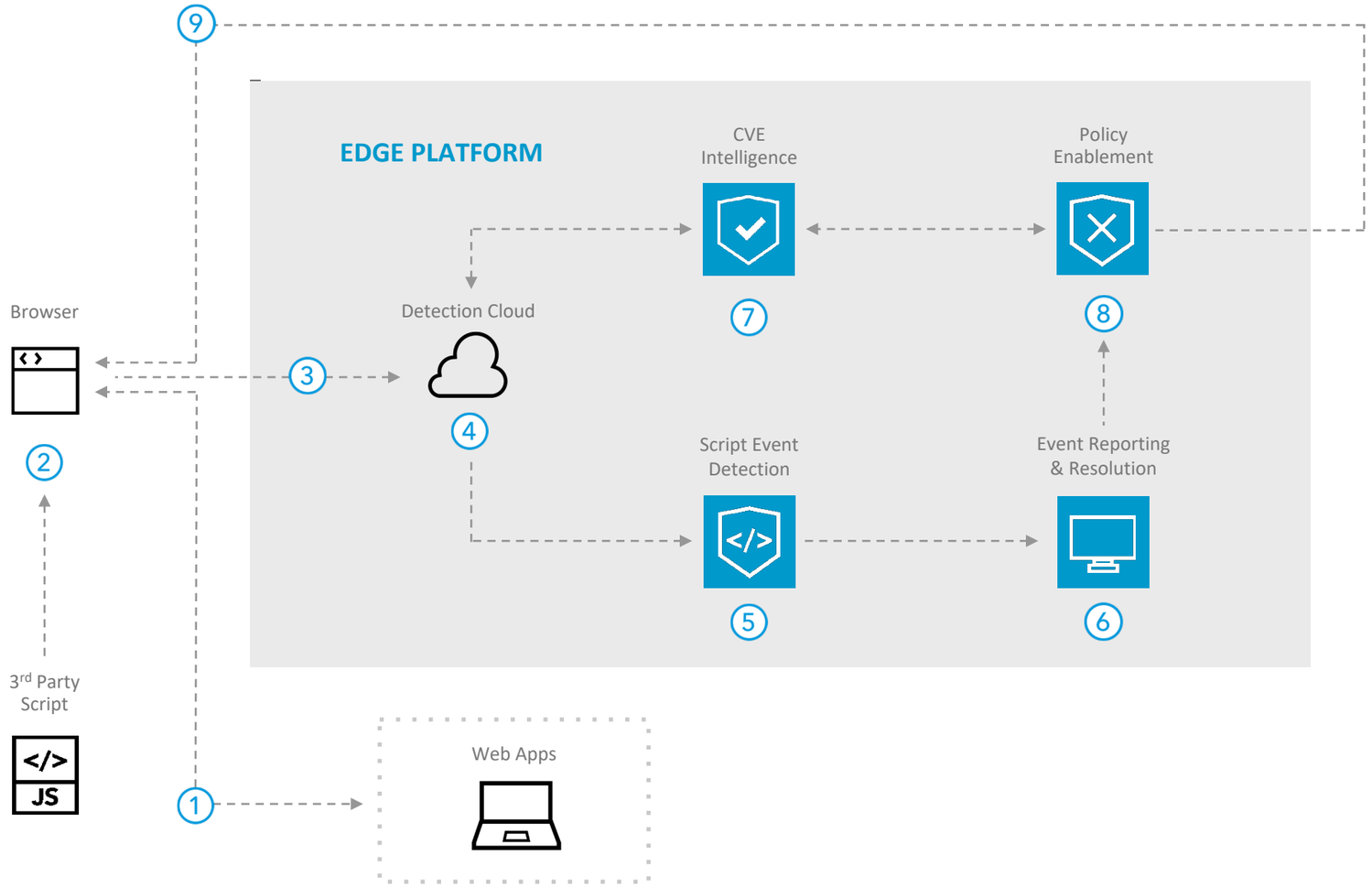
Client-Side Protection & Compliance

Reference Architecture



OVERVIEW

Client-Side Protection & Compliance provides a behavioral approach to script protection designed to detect malicious script activity, protect the integrity of your web pages, and safeguard your business.

1. Via popular browsers, users access web page functions from a web app–generated HTML page that includes an average of over 100 scripts for a typical site.
2. Over half of those scripts are typically requested and delivered to the browser directly from third-party partners (third-party scripts).
3. As the scripts execute in-browser, Akamai sends execution information to our detection cloud. This step looks for anomalies in script behavior.
4. Suspicious anomalies are analyzed in real time and given a risk score based on a number of risk factors focused on changes in script behaviors accessing sensitive data and destination server designation.
5. Suspicious anomalies are highlighted, summarized, logged, and alerted if appropriate.
6. Security teams receive an alert indicating event severity and detailed information. If the suspicious anomaly is found to be malicious, the event can immediately be blocked, and a policy can be created.
7. In parallel to anomaly detection, collected script data is compared against Akamai Common Vulnerabilities and Exposures (CVE) intelligence to find security gaps and weaknesses.
8. Found CVE weaknesses are identified and can be added to Client-Side Protection & Compliance policies to continuously block inappropriate exfiltration of sensitive data.
9. From threats detected by script protection, outgoing policies prevent sensitive information exfiltration.

KEY PRODUCTS

Script Protection ▶ Client-Side Protection & Compliance

Published 10/23