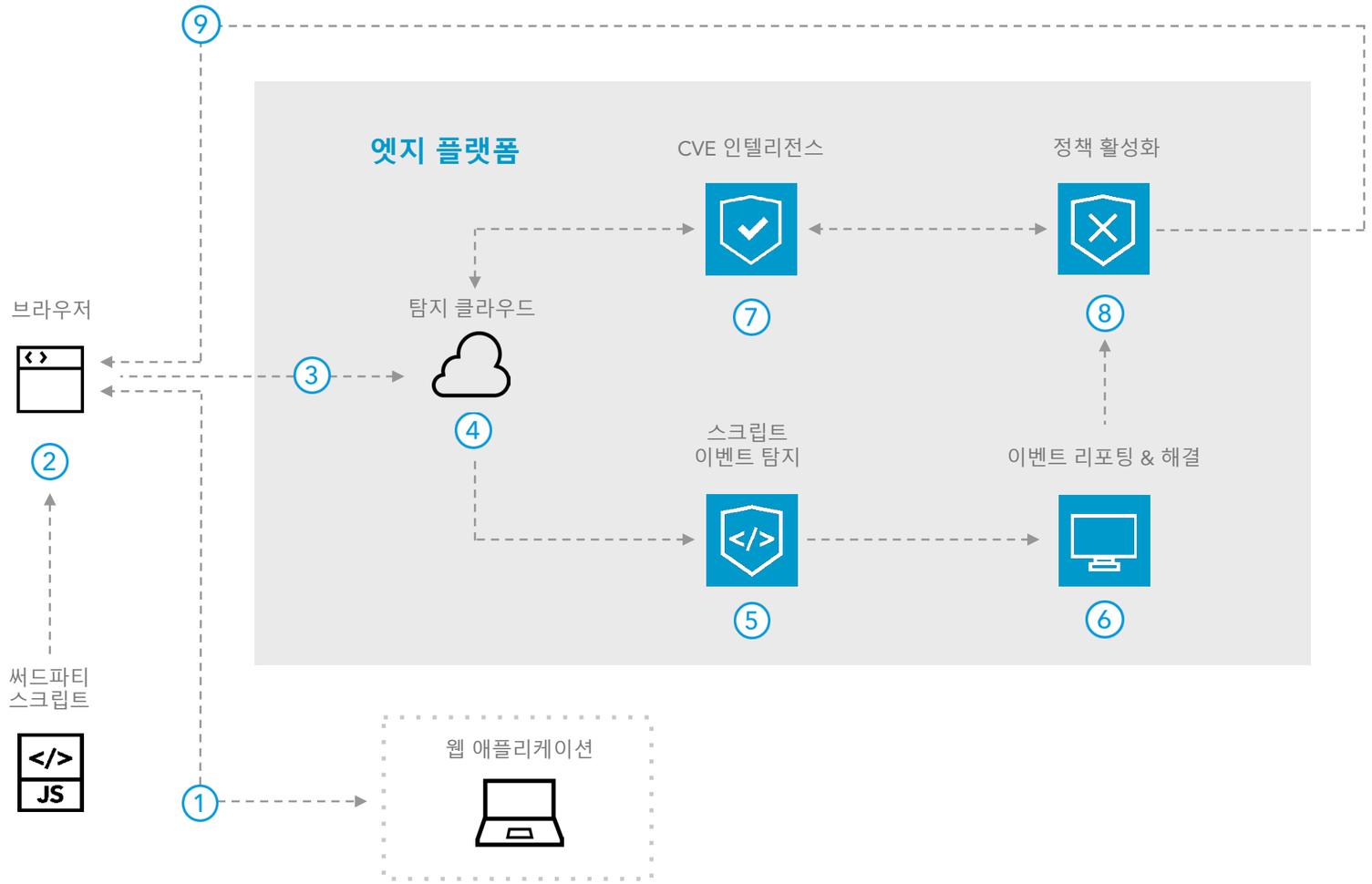
Client-Side Protection & Compliance

레퍼런스 아키텍처



개요

Client-Side Protection & Compliance는 행동 기반의 접근 방식을 스크립트 보안에 적용해 악성 스크립트 활동을 탐지하고 웹 페이지의 무결성을 보호하며 비즈니스를 안전하게 보호합니다.

1. 사용자는 널리 사용되는 브라우저를 통해 일반적인 사이트의 경우 평균 100개 이상의 스크립트를 갖고 있는 웹 애플리케이션에서 생성된 HTML 페이지에서 웹 페이지 기능에 접속합니다.
2. 이러한 스크립트의 절반 이상은 일반적으로 써드파티 파트너(써드파티 스크립트)가 직접 요청해 브라우저에 전달합니다.
3. 스크립트가 브라우저 내에서 실행되면 Akamai는 실행 정보를 탐지 클라우드로 전송합니다. 이 단계에서 비정상적인 스크립트 행동을 찾습니다.
4. 비정상으로 의심되는 행동을 실시간으로 분석하고 민감한 데이터와 대상 서버에 접속하는 스크립트의 행동 변화에 중점을 둔 여러 개의 리스크 요소를 기반으로 리스크 점수를 책정합니다.
5. 의심스러운 비정상은 강조 표시, 요약, 기록되고 적절한 알림이 전송됩니다.
6. 보안팀은 이벤트 심각도와 자세한 정보에 대한 알림을 받습니다. 의심스러운 비정상이 악성으로 판명되면 즉시 이벤트를 차단하고 정책을 생성할 수 있습니다.
7. 비정상 탐지와 동시에 수집된 스크립트 데이터를 Akamai의 CVE(Common Vulnerabilities and Exposures) 인텔리전스와 비교해 보안 격차와 취약점을 찾아냅니다.
8. 발견된 CVE 취약점을 식별하고 Client-Side Protection & Compliance에 추가해 민감한 데이터의 부적절한 유출을 지속적으로 차단할 수 있습니다.
9. 스크립트 보안 기능이 탐지한 위협을 기반으로 정책을 통해 민감한 정보의 유출을 방지합니다.

주요 제품

스크립트 보안 ▶ Client-Side Protection & Compliance

2023년 10월 발행