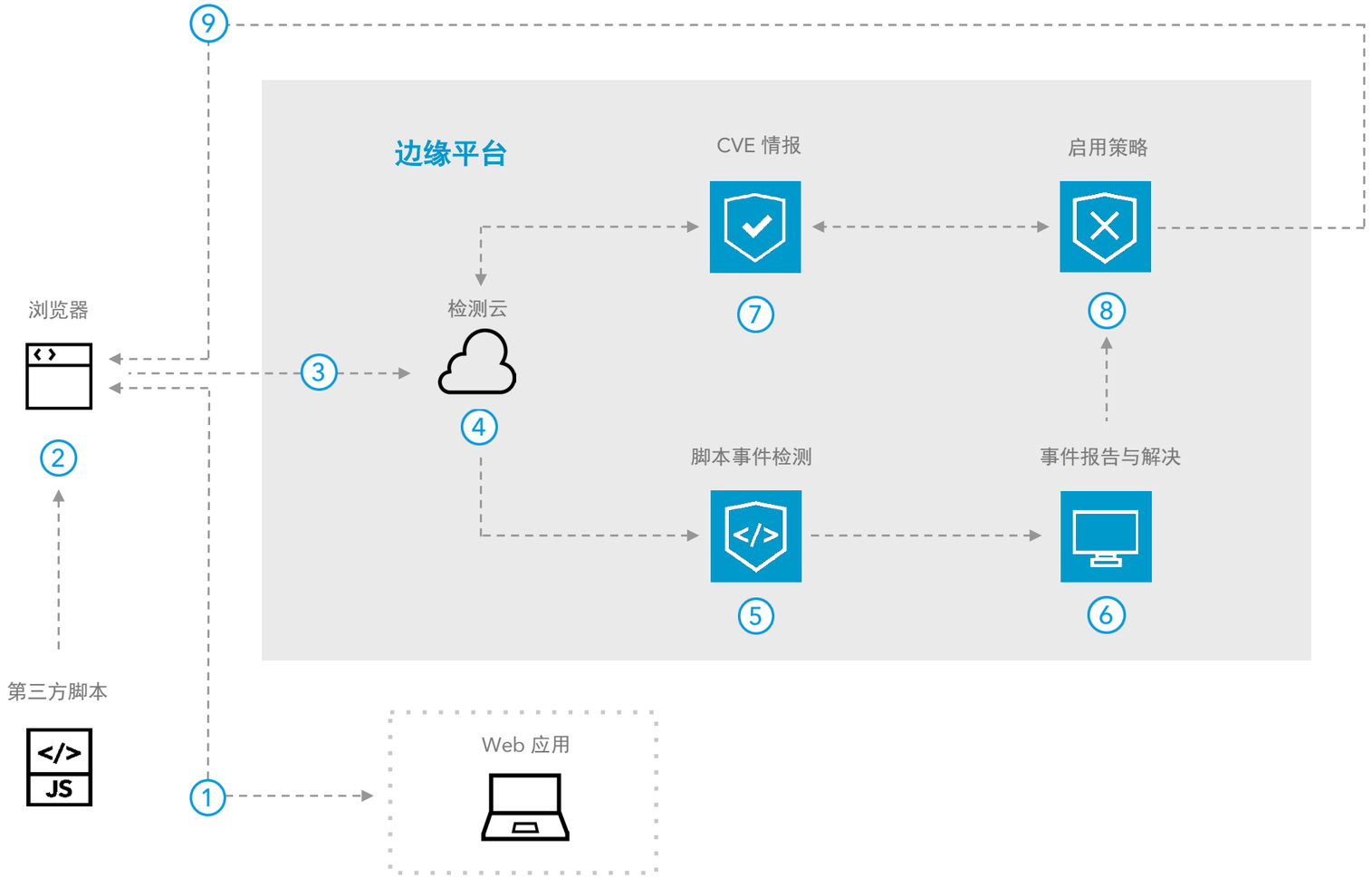
Client-Side Protection & Compliance

参考架构



概述

Client-Side Protection & Compliance 提供了一种采用行为技术的脚本保护功能，旨在检测恶意脚本活动、保护网页的完整性并保护您的业务。

1. 用户通过一些常用浏览器，在 Web 应用程序生成的 HTML 页面上访问 Web 页面功能，对于典型站点，此类页面平均包含超过 100 多个脚本。
2. 通常，这些脚本中有半数以上直接通过第三方合作伙伴（第三方脚本）请求并提供给浏览器。
3. 当脚本在浏览器内执行时，Akamai 会将执行信息发送到我们的检测云。此步骤会查找脚本行为中是否存在异常。
4. 实时分析可疑的异常行为，并根据诸多风险因素，特别是访问敏感数据和目标服务器名称的脚本行为的变化，给出风险评分。
5. 突出显示、汇总和记录可疑的异常问题，并在适当时发出告警。
6. 安全团队将收到表明事件严重性并包含详细信息的告警。如果发现可疑异常存在恶意，安全团队就会立即阻止该事件并创建相应的策略。
7. 在执行异常检测的同时，将收集到的脚本数据与 Akamai 常见漏洞和风险 (CVE) 情报进行比较，以查明其中是否存在安全漏洞和弱点。
8. 如果发现 CVE 漏洞，系统将会对其进行识别并添加到 Client-Side Protection & Compliance 策略中，以持续阻止敏感数据的不当泄露。
9. 根据脚本保护机制检测到的威胁，传出策略可以防止敏感信息泄露。

关键产品

脚本保护 ▶ Client-Side Protection & Compliance

发布时间：2023 年 10 月