AKAMAI 产品简介

Client-Side Protection & Compliance

防范客户端 JavaScript 漏洞、简化合规工作

JavaScript 是现代 Web 应用程序的重要工具。为了优化用户体验，增强功能和提升性能，第一方和第三方 JavaScript 的应用随着时间的推移呈指数级增长。使用 JavaScript 确实带来了无数好处，但 JavaScript 数字供应链也给网站留下了漏洞，让客户端攻击有机可乘。这些攻击企图通过恶意代码注入在浏览器内窃取终端用户敏感信息，包括支付卡数据。

这些攻击在服务器端无法监测，而且会绕过传统安全措施，企业很容易成为受害者，进而造成客户信任下降、高昂的监管罚款、合规处罚和品牌声誉受损。

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance 有助于防范终端用户数据泄露，保护网站免受 JavaScript 威胁侵扰。它旨在监测恶意脚本行为，并为安全团队提供可付诸行动的告警，以实时缓解恶意活动。

Client-Side Protection & Compliance 凭借专门构建且符合 PCI DSS v4.0 合规性要求的功能，能够助力企业满足新的脚本安全性要求，保护支付卡数据免受客户端攻击。您可以通过一个综合性仪表板轻松管理支付页面的脚本清单、简化审计流程，并获得专门的 PCI 告警，从而快速应对合规相关事件。

主要功能

防范客户端的敏感数据泄露

网络犯罪分子在寻找您终端用户的敏感信息。他们会利用 JavaScript 供应链中的漏洞，将恶意代码注入网站，从而窃取敏感信息，并将其用于欺诈目的。Client-Side Protection & Compliance 整合了机器学习与启发式评分技术，可实时分析脚本行为，以检测恶意活动和存在漏洞的资源。它能立即为安全团队提供可付诸行动的告警，支持其迅速抵御客户端攻击，包括 Web 数据窃取、Maegecart 和表单劫持。

对企业的好处

检测和保护 监控真实用户会话中的脚本行为，检测可疑活动

PCI DSS v4.0 工作流
帮助满足第 6.4.3 和 11.6.1 条中的 JavaScript 安全要求

优先级清晰的实时告警
通过可辅助行动的告警立即抵御高风险事件

客户端监测能力
获得丰富的视图，了解客户端攻击面的各种信息

策略管理
治理脚本行为，控制运行时 JavaScript 执行

漏洞检测
在 Akamai 威胁情报的支持下识别常见漏洞与风险 (CVE)

灵活的部署选项
部署轻而易举，可通过 Akamai Connected Cloud 部署，也可直接在源站服务器上部署

Akamai

满足专门的 PCI DSS v4.0 合规性要求

依据 PCI DSS v4.0 脚本安全性要求的第 6.4.3 和 11.6.1 条，企业要为支付卡数据提供客户端攻击防护机制，并确保对支付页面上的脚本进行管理。Client-Side Protection & Compliance 会跟踪并清点支付页面上的所有脚本，确保其完整性和授权。它提供预定义的合理性证明和自动化规则，可轻松证明所有已加载脚本的合理性。该解决方案还会监控 HTTP 标头和支付页面保护机制中的变更，防范网页篡改。综合性仪表板和专用 PCI 告警让企业能够快速响应合规相关事件，妥善保护浏览器内的支付卡数据。利用这些功能，安全和合规团队即可降低 PCI 审计流程的负担，并快速简化工作流。

对 JavaScript 威胁的广泛监测能力

传统 Web 应用程序保护措施（如 Web 应用程序防火墙）仅监控服务器端流量，无法监测在客户端执行的活动。防范此类威胁的基于标准的方法（比如内容安全策略）难以管理，在抵御供应链内超出网页运营者控制范围的脚本引入的恶意攻击载荷方面，保护能力较为有限。这就给企业造成了盲点，让恶意代码可以潜藏长达数天、数周乃至数月，并在此期间持续窃取敏感数据。Client-Side Protection & Compliance 可提供有关网站客户端攻击面的出色视图，包括各脚本行为、漏洞、覆盖范围和影响力，以及所访问过的数据或遭遇过的威胁。

工作原理

Client-Side Protection & Compliance 在终端用户浏览器内运行，监控客户端脚本在受保护网页上的执行情况。在脚本行为发生变化时，它将使用机器学习技术来评估未经授权或不当的操作所带来的风险。如果遇到高风险事件，它会向安全团队发出告警，使其能够立即着手调查潜在威胁，并实施抵御方案。

设置在所监控的每个网页中注入简单的脚本，对性能的影响几乎可以忽略不计。

监控和评估从用户的网页浏览器中收集 JavaScript 活动数据，并监控这些数据。利用机器学习技术，评估未经授权或不当行动（如发现此类行动）的风险。

告警在发现活跃威胁或攻击时，发送实时告警，并提供详尽的信息，以帮助抵御威胁。

缓解只需轻松点击一下，就能立即对恶意 JavaScript 脚本实施限制，禁止其访问和泄露受保护网页中的敏感数据。

加快满足 PCI DSS v4 脚本安全合规要求的步伐

脚本完整性和授权 (6.4.3)

确保受保护支付页面上加载的所有脚本的完整性和授权。

脚本清点和合理性证明 (6.4.3)

跟踪并清点受保护支付页面上加载的脚本。利用预定义的合理性证明和自动化规则，快速证明所有脚本的合理性。

支付页面保护 (11.6.1)

立即检测并应对受保护支付页面上未经授权的更改。

直观易懂的仪表板

专用仪表板提供脚本安全要求第 6.4.3 和 11.6.1 条相关任务和告警的详细信息，简化 PCI DSS v4.0 合规和审计流程。

可付诸行动的 PCI 告警

接收并记录 PCI 合规相关事件的详细告警，包括未经授权的脚本、支付数据泄露和支付页面篡改。

如需了解更多信息，请访问我们的产品页面或联系 Akamai 销售团队。