AKAMAI 检查清单

借助 Akamai Client-Side Protection & Compliance，拥有 PCI DSS v4.0 JavaScript 安全检查清单

支付卡行业数据安全标准 (PCI DSS) 是一项全球安全标准，旨在保护支付卡的在线数据安全性，并促进在全球范围内广泛采用一致的数据安全措施。这是最重要的安全标准之一，在线处理支付卡数据的所有企业都必须遵守此项标准。

PCI DSS 的最新版本（仅有英文版）为 4.0 版，将于 2025 年生效。它包含 12 项核心数据安全性要求，并提供了应对新型及不断发展演进的网络安全威胁的最新指导。PCI DSS v4.0 中新增了两条重要要求（第 6.4.3 条和第 11.6.1 条），分别涉及 JavaScript 安全性及防范客户端 Web 数据窃取攻击，此类攻击可从浏览器内窃取敏感的最终用户信息。历经多年发展，这些攻击日渐普遍，而复杂的技术也导致其隐匿性越来越强。它们可能给受害企业造成破坏性极大的后果——包括高昂的罚款、品牌声誉受损、收入损失和客户信任下降。

我们来看一下全新 PCI DSS v4.0 脚本安全要求的检查清单，以及 Client-Side Protection & Compliance 如何满足这些要求。

PCI DSS v4.0 要求	Client-Side Protection & Compliance 提供帮助的方式
第 6.4.3 条要求——保护面向公众的 Web 应用程序，使其免受攻击 ☑ 实施了一种方法，确认浏览器内加载和执行的每个脚本均经过授权 ☑ 实施了一种方法，确保浏览器内加载和执行的每个脚本的完整性 ☑ 维护浏览器内所加载和执行的所有脚本的清单，并提供各脚本必要性的书面证明	**一键即可轻松授权** ☑ 直接在工具内轻松管理允许在您网站的支付页面上执行的脚本 **预先确保完整性** ☑ 行为技术对浏览器内执行的每个脚本进行分析，以检测恶意活动或数据泄露，并就此发出告警 **自动跟踪和清点所有脚本** ☑ 预定义的理由和自动化规则可轻松证明浏览器内加载和执行的每个脚本的用途

PCI DSS v4.0 要求	Client-Side Protection & Compliance 提供帮助的方式
第 11.6.1 条要求——检测并响应未经授权的支付页面变更 **按如下方式部署变更检测和篡改检测机制：** ☑ 向相关人员发出告警，提醒其注意消费者的浏览器接收到的 HTTP 标头和支付页面内容遭到未经授权的修改（包括入侵、更改、添加和删除的指标） ☑ 此类机制配置为评估所收到的 HTTP 标头和支付页面 **此类机制**至少每七天运行一次或者定期运行（按照实体的定向风险分析确定的频率运行，此分析根据第 12.3.1 条要求中指定的所有元素执行）	**保护您的支付页面** ☑ 监控、分析和抵御对支付页面的恶意篡改，确保最终用户的宝贵数据安全无忧 **提供具备可操作性的即时告警，支持实时调查未经授权的修改** ☑ 借助即时检测功能，安全团队可对支付页面上未经授权的 HTTP 标头更改或修改做出快速应对 **通过始终开启的防御机制实施保护** ☑ 全天候保护机制保证用户在支付页面上的交互安全无虞

Akamai Client-Side Protection & Compliance 提供针对 JavaScript 威胁的可靠防护，并支持监测客户端攻击面，以保护浏览器内的敏感数据。专门构建的 PCI DSS v4.0 功能可帮助安全和合规团队简化 PCI DSS v4.0 审计流程，并提供专用工作流来帮助满足脚本安全要求中的第 6.4.3 条和第 11.6.1 条。

Akamai Client-Side Protection & Compliance 具备灵活的部署选项，不要求启用 Akamai Connected Cloud。

进一步了解这些功能如何帮助贵公司遵从 PCI DSS v4.0 的要求。

 | 支持 | 发布时间：2023 年 9 月

扫码关注，获取最新CDN前沿资讯