AKAMAI 解决方案简介

Akamai 帮助金融机构做好 PCI DSS 合规准备

PCI DSS v4.0 为支付卡行业安全标准带来了自 2004 年以来最重大的变化，金融机构必须迅速适应以保持合规性。PCI 安全标准委员会制定的这一综合框架要求采取严格措施来保护持卡人数据。Akamai 的解决方案提供先进的安全功能、持续监控和强大的渗透测试，使金融机构能够满足这些不断变化的要求。我们的工具旨在简化合规流程、保护客户信息，并帮助您的机构在 PCI 2025 年 3 月截止日期之前做好准备。

统一合规性：一家供应商即可简化 PCI DSS

对于金融机构而言，PCI DSS 合规性不仅涉及员工培训和企业政策，还需要复杂的安全软件来满足大多数要求。鉴于这些要求的综合性，这往往意味着要与多家供应商合作。有些要求可能需要防火墙，还有一些要求可能需要身份管理。如果能找到一家集各种技术于一身的提供商，金融机构就能简化审计流程，更好地保护客户财务信息安全。作为更广泛安全战略的一部分，采用能满足这些要求的强大网络安全解决方案，从长远来看可以节省成本并降低复杂性。Akamai 的解决方案组合全面满足现有和即将出台的 PCI DSS 要求，可为金融机构提供无缝体验。

解决范围问题

希望满足 PCI DSS 要求的金融机构面临一个重大挑战，那就是范围问题。规属在 PCI“范围内”的应用程序和网络环境复杂，涉及各种不同类型的基础架构、技术和位置。随着越来越多的金融机构将基础架构和基于 SaaS 的应用程序转移到云端，这种本地部署与按需部署服务共存的混合环境让问题变得更复杂。对于金融机构而言，他们很难随时了解特定的工作负载位于何处，那些拥有自动扩缩电商业务的机构亦是如此。

为此，金融机构希望通过内部防火墙、VLAN 和访问控制列表来应对范围带来的挑战。然而，这些传统应用程序往往很难满足混合环境的要求，而且还会带来安全漏洞，增加复杂性、停机时间和运营开销。

优势

- **简化安全和合规工作流程**
- **利用专用 PCI 功能减轻审计负担**
- **接收并记录切实可行的 PCI 合规告警**
- **保护敏感财务数据**
- **提高运营效率并降低合规成本**

Akamai Guardicore Segmentation 可监测持卡人数据环境 (CDE) 及其边界，这是合规流程中的一个关键步骤。这种监测能力有助于金融机构满足 PCI DSS 中的多项要求并对机构网络进行全面监督。例如：

- 第 1.2.3 条要求规定，企业应拥有自己的网络图。Akamai Guardicore Segmentation 的仪表板可清晰展示 CDE 与其他网络之间的所有关联，从而帮助金融机构满足该要求。
- 第 1.2.4 条要求规定，企业应维护数据流程图，以指明帐户数据在系统和网络中的移动情况。Akamai Guardicore Segmentation 的仪表板可以通过展示必要的关联来帮助金融机构满足该要求。

解决控制问题

- 第 1.2.5 条要求规定，企业有必要识别所有服务、协议及端口的信息，对其进行审批并有明确的业务理由许可使用它们。Akamai Guardicore Segmentation 可帮助金融机构满足该要求，它可以采取通用策略来确定允许和不允许使用的协议或服务。

解决客户端保护问题

对接受支付卡数据的金融机构而言，他们不能仅对自己的环境负责。虽然 JavaScript 在现代 Web 开发中的应用带来了创新，提高了连贯性，但也给支付卡处理商带来了很多挑战。JavaScript 分散运行在各个客户端上且依赖于第三方提供，因此金融机构想要监控和管理 JavaScript 就变得极为困难。攻击者正是利用了这一盲点，向客户端的网站注入有害代码以窃取敏感数据。诸如 Web 数据窃取、表单劫持和 Magecart 之类的攻击日渐增多，促成了事关客户端保护和脚本监控方面的新要求。

PCI DSS v4.0 要求金融机构必须对其面向公众的网站的支付页面上执行的所有 JavaScript 进行跟踪和盘点，并证明有合理的理由执行它们。第 6.4.3 条要求规定，企业必须确保所有脚本的行为完整性和授权，还要提供这些脚本的清单以及有关执行各脚本的必要性的书面证明。另外，第 11.6.1 条要求规定，金融机构需要检测其支付页面上是否具有任何未经授权的变更，并采取相应的应对措施。一旦发现消费者的浏览器接收到的 HTTP 标头和支付页面内容遭到任何修改，包括具有遭到入侵、更改、添加和删除的迹象，企业必须向授权人员发出告警。

> 借助 Akamai Guardicore Segmentation，我们大大缩小了攻击面，而且没有产生与升级传统防火墙相关的成本和延误。
>
> ——**Dave Wigley**
> **Daiwa Capital Markets Europe**
> **首席信息安全官**

总而言之，PCI DSS v4.0 要求金融机构：

- 盘点支付页面上执行的所有脚本，并证明其合理性
- 确保所有脚本都获得了授权，并执行预期的操作
- 建立检测、告警和响应机制，以应对支付页面遇到的未经授权的脚本变更、保护机制篡改和数据外泄问题

Akamai Client-Side Protection & Compliance 可提供广泛的支持，助力金融机构满足 PCI DSS v4.0 中的第 6.4.3 条和第 11.6.1 条要求。该解决方案会自动跟踪并清点支付页面上的脚本，确保其完整性和授权。安全团队可以通过预定义的依据和自动套用的规则，轻松判定支付页面上所执行脚本的目的。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，以防范网页遭篡改。借助综合仪表板和专门的 PCI 告警，安全团队可以轻松快速地应对合规相关事件，并为审计提供证据。

防范攻击

保护持卡人数据是 PCI DSS 的核心原则，但随着 Web 应用程序和 API 的激增，它们也成为攻击者的突破口。为了遵守 PCI DSS 要求，金融机构需要强大的保护机制来抵御恶意软件、零日攻击以及其他可能导致数据泄露的威胁。

Akamai App & API Protector 及其 Malware Protection 模块可以在网络边缘扫描文件，提前阻止恶意软件进入网络内部并开始传播，从而帮助金融机构避免支付卡信息发生数据泄露。API 的普及也暴出了新的漏洞，让伺机收集支付卡数据的攻击者有机可乘。许多金融机构甚至无法说明其所有 API 的用途，更不必说证明它们的安全性了。所有接收或传输持卡人数据的 API 都在 PCI DSS 的合规性要求范围内，因此，金融机构需要监控 API 的开发和身份验证并确保它们的安全。

Akamai API Security 可自动持续发现您环境内的 API。该应用程序可将这些 API 与现有文档进行对比，并将发现的错误配置和漏洞报告给安全团队、开发人员和 API 团队，然后给出相关 API 和端点的风险评分。这是一个持续自动执行的过程，因此在您完成 API 资产更新时，该应用程序会对漏洞进行评估。

结论

虽然实施 PCI DSS 控制的最终目标是保护持卡人数据，进而达到保护您的客户和业务的目的，但金融机构仍然需要满足审计人员的要求。而使用单一的提供商具有显而易见的优势。凭借有关您网络的实时数据和历史数据，您可以更快、更轻松地满足诸多方面的审计要求。此外，您应选择一家在此领域具有优势地位的提供商，且其拥有稳定的客户群体已成功达到 PCI DSS 要求。与这样的提供商合作可以帮助您更顺利地实施相关控制、更快完成审计，并且持续提供合规支持。Akamai 全面的监测能力和集成的解决方案可帮助金融机构简化合规工作并加强对不断演变的威胁的防御能力。

如需了解更多信息，请访问 akamai.com 或联系您的 Akamai 销售团队。