AKAMAI 解决方案简介

通过 Akamai 实现 PCI DSS v4.0 合规性

PCI 合规性是指遵守一套全球性的安全要求，以保护和确保涉及支付卡帐户数据的各种环境的安全。任何在线处理、传输或存储持卡人数据的企业都有责任遵守支付卡行业数据安全标准 (PCI DSS)。该标准于 2004 年制定并会定期进行更新，以应对行业变化和不断演变的网络安全威胁。最新标准 PCI DSS v4.0 于 2022 年 3 月发布并且内容做了重大调整，其中包含企业需要在 2025 年 3 月之前满足的 12 项核心要求。

做好迎接 PCI DSS v4.0 的准备了吗?

虽然不遵守 PCI 标准不会受到法律的惩罚，但信用卡公司可以对不遵守该标准的企业进行罚款。此外，如果不具备确保持卡人数据安全的能力，相应品牌便会非常容易受到网络攻击，进而导致毁灭性的数据泄露，造成巨额罚款并永久丧失客户信任。

我们将随时为您提供帮助。Akamai 不仅保持 PCI DSS 1 级合规性，还提供各种出色的安全解决方案，帮助企业满足 PCI DSS v4.0 合规性要求。有些解决方案甚至有助于减少 PCI 审计的范围，从而节省花费在满足认证要求上的宝贵时间和金钱。

App & API Protector（含 Malware Protection 附加模块）

保持日志合规性并防范个人身份信息数据泄露、零日攻击、CVE 以及其他基于边缘的攻击，以符合 6.4.2、6.5.3 和 11.5 项要求。

> “现有恶意软件程序数量已经超过 10 亿个，而每天都会检测到 560,000 个新的恶意软件。”
>
> 资料来源：Getastra | 30+ Malware Statistics You Need to Know In 2023

API Security

检测 API 行为并减少逻辑滥用，记录 API 活动并为您的 API 实施响应式自动保护，以帮助满足合规性要求 6.2.3、6.2.4、6.3.2、6.4.1、6.4.2、10.2.1、10.5.1 和 11.3.2。

> “到 2024 年，API 滥用和相关数据泄露将几乎翻一番。”
>
> 资料来源：Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs（仅提供英文版本）

优势

- **简化安全团队和合规团队的工作流程**
- 通过专门构建的专用 PCI 功能，**减轻审计负担**
- 针对合规性事件，**接收并记录可作为行动依据的 PCI 告警**
- 利用 Akamai 全面的安全解决方案组合**整合供应商**以满足 PCI 要求

Client-Side Protection & Compliance

通过帮助防范 Web 数据窃取或 Magecart 等客户端攻击（这些攻击通过在浏览器中执行的恶意代码注入从线上结帐页面窃取并泄露支付卡数据）来满足新的 JavaScript 安全要求 6.4.3 和 11.6.1。

> **“2022 年，有 81% 的大型在线零售商报告其企业遭受过可疑脚本行为的攻击。”**
>
> 资料来源：From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 （仅提供英文版本）

Akamai Guardicore Segmentation

通过利用集成在单个平台中的多种技术，以更高效的方式对受监管资产进行分段，帮助满足多项 PCI 要求。获得网络和资产监测能力、分布式防火墙、直至第 7 层的策略实施以及入侵检测与响应。

> **“软件定义的分段使我们能够在进程级别创建和实施分段策略，从而显著改善安全态势并提高满足 PCI-DSS 技术要求的能力。”**
>
> — Senior Infrastructure Engineer, The Honey Baked Ham Company

要进一步了解如何通过 Akamai 加快实现 PCI DSS v4.0 合规性，请联系我们的专家团队。

扫码关注 · 获取最新CDN前沿资讯