CLOUDFLARE

白皮书

维持 PCI DSS 4.0 合规的战略性方法

目录

概述

所有处理信用卡、借记卡或预付卡的组织都必须遵守支付卡行业数据安全标准 (PCI DSS)。其中包括小商户、零售商、电子商务网站、银行和大型企业。然而，随着向云端和混合工作模式的转变，再加上标准不断演变，例如 PCI DSS 4.0 推出，使得高效合规变得困难。

在这个数字现代化的世界中，需要一种全新方法来以可扩展的方式简化合规流程，使组织跟上企业数字现代化的步伐，同时应对不断变化的监管环境。

当今组织面临的 PCI DSS 合规挑战

PCI 合规至关重要，违规者将面临罚款、诉讼和政府调查。然而，合规要求对金融机构、电子商务商家和其他受其监管者构成了一些挑战。

鉴于 IT 团队因更多地依赖云计算和远程办公而失去对数字环境的控制，解决这些挑战的过程变得更加复杂。

时间和资源分配： 53% 的组织表示技术隐私角色人手不足，使合规更具挑战性。[1]

多样化环境中的数据安全： 随着云计算和移动支付的兴起，在多样化且常常缺乏控制的环境中确保合规日益困难。

技术堆栈集成的复杂性： 集成和维护必要的技术以满足合规标准，例如加密和防火墙配置，通常是复杂的。对于拥有传统系统或正在进行数字转型的组织而言，这项挑战更加严峻。

审计： IT 团队必须对所有基础设施和系统中保持最新的审计跟踪，以确保合规。

供应商合规： 确保第三方服务提供商和供应商符合 PCI 标准增加了另一层复杂性。

通过 PCI DSS 4.0 跟上应对复杂网络威胁的步伐

PCI DSS 4.0 于 2022 年 3 月 31 日发布，于 2024 年 3 月 31 日生效，额外要求将于 2025 年 3 月 31 日生效。PCI DSS 4.0 的目标是：[2]

1. 继续满足支付行业的安全需求

- **加强身份验证要求：**更加强调身份验证，特别是对所有进入持卡人数据环境 (CDE) 的访问进行多因素身份验证 (MFA)。密码要求也更加严格，从最小 8 个字符增加到 12 个字符。
- **更强的加密要求：**PCI DSS 4.0 要求对存储和传输持卡人数据使用“强大”的加密，例如不易受已知漏洞利用的 TLS。
- **为应对当前威胁的新电子商务和防网络钓鱼要求：**PCI 4.0 有针对客户端安全和防范网络钓鱼和社会工程攻击的额外要求。

2. 促进安全成为持续的过程

- **更加注重风险分析和管理：**组织被鼓励实施持续的风险分析和管理流程，及时识别和解决漏洞。
- **更加强调责任和治理：**新版本更加注重持卡人数据的治理和对维持安全控制的责任。
- **有关实施和满足安全要求的更多指引：**PCI 4.0 澄清了标准的意图和使用的时间框架。

3. 增加对不同方法的灵活性

- **集成新技术：**PCI DSS 4.0 解决新兴技术的安全性，例如云和移动支付系统。
- **组织实现安全目标的方式更灵活：**组织可以采用“定制方法”，通过更广泛的方法来满足要求。PCI 4.0 提供更多灵活性，根据针对性的风险分析确定他们执行操作的频率。

4. 加强验证方法

- **持续监控和测试：**新标准鼓励从年度合规验证转向持续的安全和合规监控。
- **评估和合规声明之间更加一致：**自评问卷或合规报告中的信息与合规声明中总结的内容更加一致。

解决方案：通过 Cloudflare 全球连通云满足 PCI 合规要求的新方法

安全和 IT 团队需要以简单、可编程的方式处理 PCI 要求，这种方式可以轻松与其现有的安全和技术堆栈集成，并随着他们的基础设施和 PCI DSS 的演进保持这种状态。

答案不是拼凑多种传统和单点安全解决方案的方式。相反，团队需要一个统一的云原生安全和网络服务平台，其宗旨是帮助企业重新控制其 IT 环境，并满足包括 PCI 在内的各种合规要求。这样的统一平台被称为“全球连通云”。

全球连通云提供：

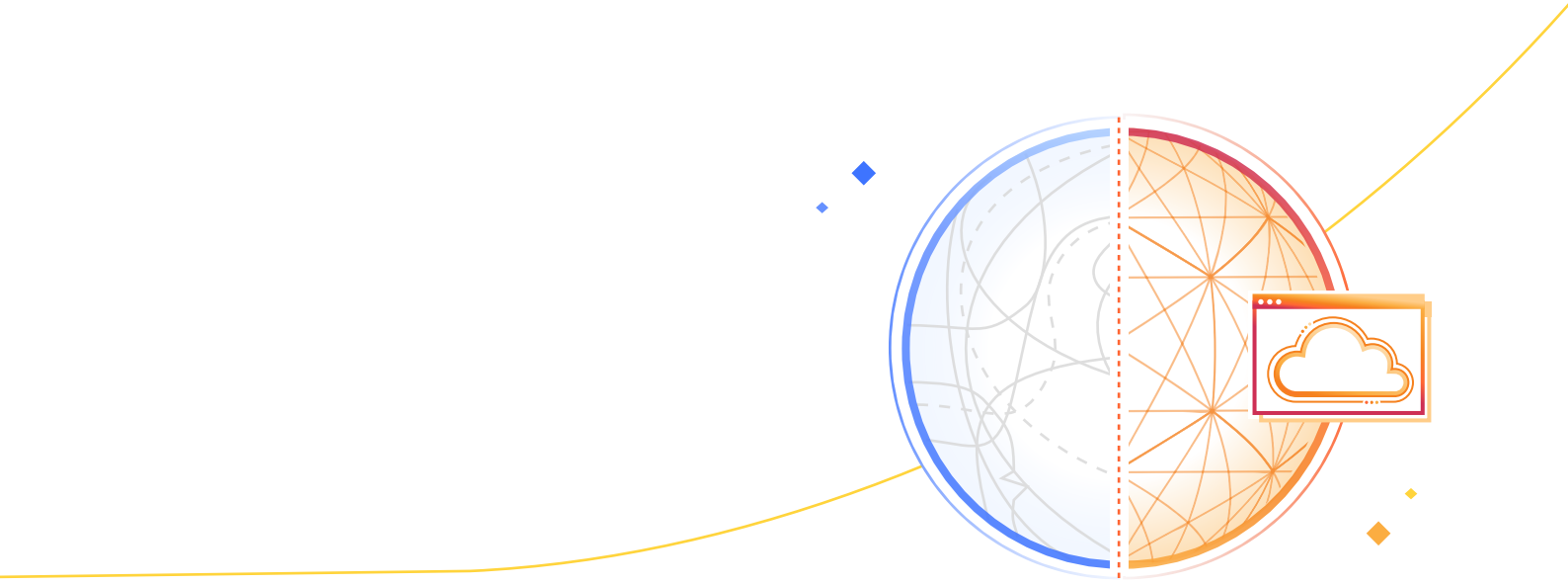
- 一个专为数据合规而设计的平台
- 一个统一的策略引擎
- 毫不妥协的数据主权
- 满足审计要求的智能报告

Cloudflare 允许 IT 团队在各个地点应用一致的控制，使用单一的控制平面在所有地方激活控制。

团队可以直接从 Cloudflare 边缘将日志发送到首选的 SIEM 或云目的地以供审计。此外，Cloudflare 具备对互联网流量的大规模可见性，因而能够自动识别并防御新威胁。

Cloudflare 本身符合 PCI 标准，并原生支持 PCI DSS 4.0 要求。例如，Cloudflare 使 IT 团队能够轻松实施多因素身份验证，这是 PCI DSS 4.0 的重点要求之一。Cloudflare 还支持最新的加密标准，并经常为其做出贡献，帮助客户满足 PCI DSS 4.0 有关敏感信息加密的要求。

下一页是 PCI DSS 要求与 Cloudflare 全球连通云能力之间的简要对照：



Cloudflare 可帮助解决 PCI 要求的关键领域*

PCI 要求	Cloudflare 能力
1. 安装和维护网络安全控制（以前是“安装和维护防火墙”）。	Cloudflare 保护网络、应用程序和云部署，防范恶意网络流量。Cloudflare 利用源于每天数百亿个威胁的威胁情报，保护网站和 Web 应用程序免受 Web 威胁侵害，包括 OWASP 十大风险和 zero-day 攻击。Cloudflare 的云原生安全平台可在数分钟内部署到位，并允许用户在几秒钟内推出全球策略更改。
2. 对所有系统组件应用安全配置。	在 Cloudflare 后面的用户、设备和应用程序都经过强加密和屏蔽，以防范潜在网络攻击。Cloudflare 的 API Shield 允许用户通过识别序列和实施围绕 API 交易的策略来创建针对其 API 中漏洞的防护措施。
3. 通过加密或其他数据保护方法保护存储的数据。	Cloudflare 可识别静态个人身份信息 (PII)，并满足持卡人日志保留时间的规定。
4. 在开放的公共网络上对持卡人数据进行加密。	通过 Cloudflare 全球网络发送的流量符合本项要求中指定的加密标准，Cloudflare 可以阻止用户需要识别的 PII 传输。
5. 保护所有系统和网络免受恶意软件的侵害。	Cloudflare 每秒处理超过 5500 万个 HTTP 请求，就实际网络环境中的最新攻击具有独特的广泛可见性。Cloudflare 为用户提供一套反恶意软件保护措施，包括防病毒、云电子邮件安全和远程浏览器隔离。
6. 开发和维护安全的系统和软件。	Cloudflare 可以对用户安全违规行为以及在 SaaS 应用程序中检测到的错误配置进行排序和权重确定。Cloudflare 的安全服务可以保护所有面向公共 Web 的应用程序免受已知攻击和利用。
7. 根据“按需知密”原则限制对持卡人数据的访问。	Cloudflare 可以执行最低权限、细粒度的访问控制，无论用户在何处或数据存储在何处。
8. 识别用户并验证对系统组件的访问。	Cloudflare 可对通过其全球网络的任何流量执行基于身份的策略和安全态势检查（例如是否使用了 MFA）。
10. 记录和监控对系统组件和持卡人数据的所有访问。	Cloudflare 在其平台上的所有产品中提供细粒度的审计日志，并与大多数主流 SIEM 集成。
11. 定期测试系统和网络的安全性。	Cloudflare 不仅提供限制访问策略测试和入侵检测服务功能，还为其所有主要产品提供深入日志记录。

* Cloudflare 不对 PCI DSS 4.0 标准的第 9 和第 12 项要求提供协助，两者涉及物理安全和组织结构。

总结：依靠 Cloudflare 帮助解决 PCI 合规要求

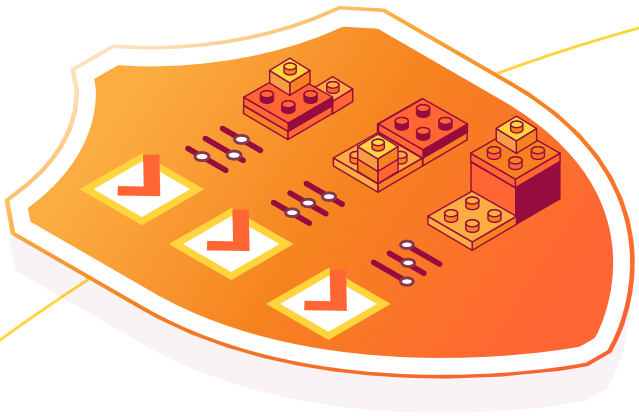
Cloudflare 符合 PCI 标准，并具有帮助客户自行解决合规要求的能力，无论其采用怎样的基础架构。

事实上，使用 Cloudflare 可将数据泄露的可能性降低 65%[3]，年度网络保险费用减少 24%[4]，管理系统和流程所需的时间缩短 59%[4]。

我们的企业客户在合同中要求 Stax 符合非常具体的合规标准。这促使我们在基础设施上实施诸如 Zero Trust 之类的安全控制……Cloudflare 完全做到了我们的要求。它保护我们的端点并确保我们的安全。” [5]

Troy Ridgewell
Stax 安全主管

STAX



欢迎了解 Cloudflare 数据合规解决方案。
联系我们的专家。

参考资料

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. IBM 2022 年度泄露成本报告
4. 2023年 Cloudflare 委托 TechValidate 进行的 Cloudflare 应用服务客户调查
5. https://www.cloudflare.com/case-studies/stax

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-5776.2024APR09