

# 医疗保健行业

API 事件频发。了解医疗保健行业如何应对 API 安全挑战，以及您可以采取哪些措施来防御不断演变的威胁。

在医疗保健行业中，患者和用户的信任至关重要。然而，API 漏洞的存在，使得医疗保健企业面临着日益严峻的安全挑战。

电子健康记录、远程医疗以及互联医疗设备已经成为网络犯罪分子的首要攻击目标，通过不安全的 API 访问受保护健康信息 (PHI) 会造成各种不良后果，如违反 HIPAA 法规、侵犯患者隐私以及破坏信任关系等。一旦失去这种信任，可能需要相当长的时间才能让患者和用户重拾信心。

这一挑战的严重程度不容忽视。在 Akamai 的一项综合调查中，有高达 84.7% 的医疗保健从业人员表示过去一年中遇到了 API 安全事件，这一数字略高于跨行业的平均值 (84%)。

但也许最令人担忧的是，这些事件对患者和用户信任造成的影响。医疗保健行业的受访者表示，API 事件发生后，“信任和声誉受损” (28.7%) 是他们最担心的问题之一。在当前的环境中，患者很容易找到其他医疗服务提供商，因而这种声誉受损不仅会直接带来损失，而且还会产生长远的影响。

继续阅读，探索 [2024 年 API 安全影响研究](#) 行业洞察。

## 随着攻击的不断增长，监测能力越来越受到关注

API 攻击会造成巨大的经济损失，为了解决这些事件，平均而言，医疗保健企业需要花费 510,600 美元。

尽管面临着这样的风险，但调查数据表明，在安全优先事项方面的差距令人担忧。在被问及未来 12 个月内的网络安全主要优先事项时，对于总共 12 个选项，“保护 API 免受攻击”排在第 11 位 (16.7%)。相反，这些企业更关注的是确保员工访问系统的身份验证安全 (24.7%) 和管理开发人员机密信息 (22.7%)。

对于医疗保健服务提供商而言，区分合法的与恶意的 API 活动仍然是个大难题。虽然在此行业中，有 65% 的受访者表示有完整的 API 清单，但其中只有 24% 的人知道哪些 API 处理敏感数据，相比 2023 年的 40%，这一数字出现了下滑。对于医疗保健企业，数据隐私不仅仅是良好实践，而且是法律的强制要求，因而这种监测能力差距会造成巨大的风险。

试想一下，如果临床部门部署了 API，但没有中心 IT 团队或安全团队采取合适的监管措施，那会发生什么情况？该 API 可能会：

- 为分享患者记录目的而构建，但没有采取正确的 HIPAA 合规性控制措施
- 系统升级之后仍处于活动状态，造成未知的接入点
- 传统安全工具在检测未经管理的 API 方面存在局限性，容易造成疏漏
- 被攻击者利用来访问受保护的健康信息
- 被真实合作伙伴滥用，将端点用于非计划中的用例

**84.7%** 的医疗企业在过去 12 个月内曾经历过 API 安全事件

**65%** 的医疗保健企业拥有完整的 API 清单，但其中仅有 24% 的人知道哪些 API 会返回敏感数据

**\$510,600** 这个金额表示过去 12 个月内，医疗保健企业遭遇 API 安全事件所造成的财务影响

## 三大影响

1. **信任和声誉损失** (28.7%)
2. **生产力损失** (28.7%)
3. **加强内部审查** (27.3%)

来源：  
Akamai, “API 安全影响研究”，2024 年

这些并非是危言耸听。目前医疗保健数据的泄露已经达到历史新高，而且数据泄露的平均成本为 488 万美元<sup>1</sup>，API 漏洞造成的合规性与安全风险不断加剧。此外，这种情况反映了此行业中的人员公认的 API 事件的主要成因。

## API 事件如何对合规性、业务成本以及团队压力造成影响

根据 Gartner® 2024 年 5 月发布的《API 保护市场指南》，<sup>2</sup>“当前的数据表明，平均而言，API 漏洞导致的数据泄露量至少是一般安全漏洞的 10 倍以上。”

因此，HIPAA 合规性要求越来越重视 API 安全并不令人意外。虽然 HIPAA 并未明确提及 API，但其中要求根据员工角色来限制对 PHI 的访问。这就需要对传输患者数据的 API 实施身份验证和访问控制措施。医疗保健服务提供商和保险机构及其监管机构需要掌握传输的数据类型，这不仅限于自己的 API，还包括合作伙伴和供应商的 API，这无疑增加了医疗保健领域中第三方风险管理的挑战。

失去监管机构的信任可能会导致监管机构加大审查力度，给本已疲于应对合规性要求的团队造成更大的工作压力，且可能面临高额的罚款。考虑到这一点，显然医疗保健公司非常清楚 API 威胁带来的财务后果。我们首次要求来自三个国家或地区的受访者分享他们在过去 12 个月内经历的 API 安全事件的预计成本。

|                                                                                        | 医疗保健行业     | 所有行业平均值    |
|----------------------------------------------------------------------------------------|------------|------------|
|  美国 | 510,600 美元 | 591,404 美元 |
|  英国 | 363,885 英镑 | 420,103 英镑 |
|  德国 | 643,884 欧元 | 403,453 欧元 |

问题 3：如果您经历过 API 安全事件，这些事件的累计总财务影响估值是多少？请包括所有相关费用，如系统维修、停机时间、法律费用、罚款以及其他相关费用。

尽管财务损失十分显著，但研究参与者们明确强调，其影响远超财务层面的范畴。当被问及 API 安全事件的最大影响时，如前所述，我们的受访者强调最主要的影响不是财务损失，而是“信任和声誉损失”(28.7%) 以及“生产力损失”(28.7%)。这些后果会产生长远的影响，伤害了患者的信任会损失未来数年的收入，而对于本已不堪重负的医疗保健工作人员来说，生产力损失会让人更加筋疲力尽，导致更多员工离职。

<sup>1</sup> IBM《数据泄露的代价》，2024 年  
<sup>2</sup> Gartner《API 保护市场指南》，2024 年 5 月 29 日。GARTNER 是 Gartner, Inc. 和/或其附属机构在美国和全球的注册商标和服务标志，已获许可可在本文中保留所有权利。

## 通过积极的 API 安全防护降低风险和压力

针对医疗保健公司的 API 攻击正在迅速升级，其范围、规模和复杂性不断扩大。这包括生成式 AI 驱动的爬虫程序攻击，它们能够迅速适应，并绕过传统的 API 安全工具和其他外围防御措施。许多同行的安全团队已经亲身体会到这些威胁所带来的财务和人力影响。然而，即便企业意识到了这些威胁的重要性，问题仍然摆在眼前：我们该如何应对这些威胁？

立即采取措施以更好地保护您的 API 及其交换的数据，可以帮助您的企业保护收入，减轻安全团队的压力，同时维护董事会和客户的宝贵信任。这些措施包括增强团队对高级 API 威胁的了解，并发展防御这些威胁所需的能力。



如需阅读完整报告，并了解 API 可见性与保护的 best 实践，请下载《**2024 年 API 安全影响研究**》。

准备好与我们探讨您的挑战，以及 Akamai 将如何为您提供帮助了吗？

**申请定制化的 Akamai API 安全演示服务**



Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 [akamai.com](https://akamai.com) 和 [akamai.com/blog](https://akamai.com/blog)，或者扫描下方二维码，关注我们的微信公众号。发布时间：2025 年 3 月。



扫码关注：获取最新云计算、云安全与 CDN 前沿资讯