

医疗保健行业的 API 安全性

了解 Akamai API Security 如何帮助医疗保健提供商识别并防御 API 威胁。

API 支持医疗保健提供商通过系统、设备和人员之间无缝交换数据，从而提升并优化患者护理。然而，这些数据（从患者病历到保险条款）通常具有高度敏感性，因此 API 也成为攻击者的高价值目标。

您的 API 正面临风险吗？请参考 [2024 年 API 安全影响研究](#) 中的以下调查结果：

- 近 85% 的医疗保健企业在 2024 年经历了 API 安全事件，高于 2023 年的 79%。
- 只有 24% 的企业掌握了完整的 API 清单并知道哪些 API 会交换敏感数据，较 2023 年 40% 的比例有所下降。

同时，多个行业的 IT 和安全负责人反映，为解决 API 安全事件并从中恢复，平均支出超过 94.3 万美元。

API 实现了无缝数据交换，为医疗机构带来更高互操作性与运营效率的双重优势。然而，API 也会扩大攻击面：随着 API 广泛应用于应用程序、云环境及 AI 模型中，其风险也同步上升。医疗机构往往在无意间部署了配置错误、测试不足以及缺乏访问控制的 API，使其极易被攻击者利用来窃取数据或中断运营。

Akamai API Security 帮助医疗保健提供商识别其 API 数量及其所处理的数据类型，并提供随时保护这些数据的手段。然而，许多医疗保健专业人士仍将 API 安全视为传统应用程序安全的一部分。但 AppSec 和 DevOps 人员需要将 API 的独特安全需求单独考虑。作为现代医疗保健行业的基石技术，API 带来了传统工具无法应对的全新风险。

要建立完善的 API 管理与安全计划，企业必须与正确的 API 安全服务供应商合作。在医疗保健行业，未受监控的数据流动构成重大风险，但许多企业仍缺乏一份完整的 API 清单。Akamai API Security 通过识别所有活跃 API 并分析其所处理的数据类型，帮助医疗机构全面监测其 API 环境。在此基础上，该解决方案实现持续防护，包括资产管理、敏感数据分析、异常检测、API 安全测试、CI/CD 集成，以及人工或自动修复，并可无缝集成至第三方工作流程中。

挑战



API 扩大攻击面



2024 年，近 85% 的医疗保健企业遭遇过 API 安全事件

Akamai API Security 如何应对 API 威胁

Akamai 解决方案专为医疗机构而打造，全面守护其 API 资产的安全。

全面的 API 发现

识别并清点您环境中的 API，包括 RESTful、GraphQL、SOAP、XML-RPC 和 gRPC。检测未管理或已过时、未被 API 网关涵盖的 API，并监测其属性和元数据。

理解 API 行为并检测威胁

利用 AI 驱动式分析，自动识别如数据泄露、未经授权访问、配置错误及可疑活动等安全风险。通过持续监控与异常检测，提前识别潜在威胁。

保护 API 并修复安全漏洞

实时拦截攻击，修复安全错误配置，并自动更新防火墙规则以阻止恶意流量。与现有安全生态系统（如 WAF、工单系统和安全信息与 SIEM 平台）无缝集成，增强响应能力。

部署前主动测试 API

确保在开发周期中 API 经过全面测试，进而在 API 进入生产环境之前便发现其业务逻辑缺陷、错误配置及其他漏洞。通过集成早期安全测试，企业可主动化解风险并增强 API 防护能力。

Akamai API Security

从 API 发现、风险分析，到 API 测试与合规



如需了解更多信息，请访问[我们的 API Security 页面](#)或联系 [Akamai 销售团队](#)。



扫码关注 - 获取最新云计算、云安全与CDN前沿资讯