Akamai 客户案例

财富 500 强时装行业领导者保护 API 和零售运营的安全

保护有助实现便捷、个性化零售体验的 API，同时确保客户数据不被泄露

发现所有 API

识别漏洞

提升安全态势

API 在零售业从传统实体店向电子商务平台的转型中发挥了不可或缺的作用。每一次数字交互的背后都有一个 API 在幕后助力，从而使零售商能够：

- 无缝连接各种系统、应用程序和服务
- 将他们的线上店面与后端库存管理系统、支付网关、配送服务提供商和客户关系管理工具进行整合
- 促进数据的快速交换，实现个性化且便捷的线上零售

数据保护已成为第一要务，因此 API 安全在确保线上业务运营的可信度、诚信度和机密性方面发挥着关键作用。

API 与敏感数据始终密切关联，因而成为伺机利用漏洞的网络犯罪分子眼中极具吸引力的目标。API 漏洞遭攻击者利用后，可能会导致个人详细信息、支付卡数据和购买历史记录等客户信息泄露。出于这些原因，这家财富 500 强时装零售商向 Noname Security（现已被 Akamai 收购）寻求帮助，因为该公司之前对与 Salt Security 的合作关系不甚满意。

Fashion Retailer

位置

美国

行业

零售

解决方案

Akamai API Security

Akamai

打造程序化 API 安全防护方法

这家财富 500 强零售商希望创建一个完整的端到端工作流程，以在 Web 应用程序防火墙和 API 网关之外加强对 API 安全风险的抵御。这将需要一个坚实的 API 安全防护策略，同时要采取强有力的管控措施来进行 API 管理。该公司还重视抵御爬虫程序，以最终区分合法用户和恶意爬虫程序，从而保护系统、数据和用户体验。

鉴于该项目的规模，零售商和 Akamai 一致同意采取分阶段方法。第一阶段要查找客户的所有 API，对敏感数据进行分类，实施检测和响应，并与 Splunk 进行集成。第二阶段要改为采用左移 API 安全测试方法，以加快创建安全代码。

加速部署让企业更快创造价值

尽管第一阶段任务十分艰巨，但 Akamai 团队在短短 120 天内就部署了 Noname 的 API 发现和运行时保护模块，同时执行了 Splunk 集成。API 发现在管理 API 蔓延方面起着至关重要的作用。该过程要对企业内的所有 API 进行系统化识别和编目。通过维护一个集中式 API 存储库，开发人员可以在开始新开发工作之前轻松搜索和发现现有 API。这有助于消除重复，促进重复利用，从而节省时间和工作量。

Akamai 使用基于机器学习的自动检测来识别 API 漏洞，包括数据泄露、数据篡改、数据策略违规、可疑行为和 API 安全攻击。这家财富 500 强零售商可以显著提高 API 的安全性和完整性，保护敏感数据，并保住用户和合作伙伴的信任。