Akamai 客户案例

美国某头部银行保护其 API 流量的安全并实现出色监测能力

保持严格的监管合规性，并对 API 攻击面实现了出色的监测能力

近年来，在广泛采用应用程序编程接口 (API) 的举措推动下，银行业经历了重大的转型。API 数量的这种激增使得银行可以把握新的商机，增强客户体验，以及推动业务增长。

在银行业生态系统无缝集成不同的系统和应用程序的过程中，API 发挥了极为重要的作用。银行可以通过 API 公开其服务和数据，这样就能与第三方开发人员、金融科技初创公司和其他金融机构合作，打造创新型解决方案以及扩展其产品/服务。尽管公开 API 有这些明显的优势，但同样伴随着风险。

API 安全风险会对 API 的机密性、完整性和可用性造成极大的威胁。这些风险包括未经授权的访问、注入攻击、拒绝服务攻击、不安全的数据传输、授权不足、权限升级、缺少输入验证、不安全地存储凭据以及没有足够的日志记录和监控手段。为了解决这些风险，这家领先业界的银行找到了 Noname Security（现为 Akamai 的公司）。

保持合规性

金融服务业需要遵从法规，这对于确保公正透明的商业行为、保护消费者和维护金融系统的完整性至关重要。“了解你的客户” (KYC) 和反洗钱 (AML) 等法规要求金融机构验证客户身份，评估与洗钱和恐怖主义融资相关的潜在风险，以及报告可疑活动。

Banking Leader

位置

美国

行业

金融服务

解决方案

Akamai API Security

重要影响

- 强化合规性
- 与 F5 生产环境集成
- 提供连续 API 识别

Akamai

其他法规包括支付卡行业数据安全标准 (PCI DSS)，这是一套安全标准，由主要信用卡公司制定，用以保护持卡人数据。而在金融监管方面，这些法规不过是冰山一角。因此，对于金融服务领先企业而言，了解哪些数据流经其 API 就至关重要。

公司需要改进对其 API 生态系统的整体监测能力，以便了解、管理和缓解风险，其重点在于 API 发现、数据分类、漏洞和异常检测，同时还要高度重视与其 F5 生产环境的集成。

揭示 API 使用情况

针对客户网络上往返传输以及公司内部传输的 API 流量，Noname API Security Platform（现已包括在 Akamai API Security 中）提供了监测能力。Akamai API Security 引擎会分析流量，找出金融服务领先企业的所有 API。实时流量分析可以识别新的 API 和现有 API 中的更改，并在客户仪表板上记录和更新数据。

由于该平台不依赖于任何代理或 Sidecar，并且由于它与云基础架构集成，因此该平台可以看到每个 API，不论 API 是否注册到 API 网关中。所有 API 都会被发现，包括内部和外部 API、传统 API（日期早于 API 网关）以及影子或恶意 API（没有通过网关进行路由），从而为客户提供了对其 API 攻击面的空前监测力。

展望未来

该银行业领先企业使用了一套标准来评估其 API 安全措施成功与否。其中之一是快速分类，Akamai 支持这一功能。该功能的主要目标是确定如何分析每个发现结果的严重性，这使得 SOC 可以快速评估、分类和响应告警。