Akamai 客户案例

财富 100 强零售商使用 API Security 保护数字化业务

遵循关键法规，阻断潜在的 DDoS 攻击和数据泄露途径

该零售商采用了由应用程序编程接口 (API) 的强大功能所驱动的数字化流程，正在经历重大转型。不论是运营、客户互动还是业务管理，API 均彻底改变了零售商所用的方法。

零售商纷纷通过 API，将其系统与各种第三方应用程序和服务集成，从而跨不同平台实现无缝交互。例如，通过 API，零售商可以将其电子商务平台与支付网关、配送提供商和库存管理系统集成。但是，此生态系统在扩展的过程中，也会产生大量的潜在安全漏洞。

在当今的数字化环境中，API 安全性极为重要。在连接系统、分享数据和实现集成的过程中，企业越来越依赖于 API，因此确保这些接口的安全性也就成了重中之重。有鉴于此，这家财富 100 强零售商向 Noname Security（现为 Akamai 的公司）求助，来保护其 API 攻击面。

发现 API 攻击面

API 发现在控制 API 蔓延中发挥了关键作用，API 蔓延是指企业中的 API 不受控制地激增。随着企业越来越多地采用 API 来实现数字化转型和推动创新，因此务必要采用一种系统化的方法，来有效地发现和管理这些 API。此外，在快速发展的数字化零售生态系统中，确保 API 受到保护是至关重要的第一步。

Designer Merchandise Retailer

位置

美国

行业

零售

解决方案

Akamai API Security

重要影响

- 防止数据泄露
- 发现 API 攻击面
- 降低风险和成本

Akamai

这家零售业领先企业面临的问题是，缺乏对 API 清单和流量的监测能力。公司没有针对不同平台（本地平台和云平台）的治理措施，因此无法开发可扩展的 API SDLC 保护措施。公司与我们的团队进行了交流，以期提供连续的 API 资产发现方法，用于识别错误配置、漏洞和不合规的地方，并与其现有的 SecOps 工作流（例如 Splunk）集成，从而降低风险和成本。

防止敏感数据泄露

在零售业中，企业必须遵守多种合规性法规。这些法规的目的是保护消费者权益，确保商业行为公平，以及维护数据隐私和安全。企业必须能够查看和保护用来处理敏感数据的 API，这样才能遵守关键法规和行业标准，以及避免造成法律后果和声誉受损。

Akamai 团队为这家财富 100 强零售商提供了帮助，防止数据公开暴露。该零售商曾经使用旧版本的 Jira，这带来了一个 Bug，会公开暴露员工姓名、Jira 用户名和电子邮件地址。公开的 API 同样给公司带来了安全态势风险。

Akamai API Security 解决方案可以解决公司的 API 安全态势中的这些漏洞，并修复其环境中的错误配置。例如，糟糕的架构配置为 DDoS 攻击和数据泄露提供了可乘之机，造成风险扩大。

继续推进

该客户每周都会与 Akamai 团队积极交流，来推动解决方案在企业中的采用。客户还寻求探索与其现有工作流的进一步集成。Akamai API Security 可以智能识别潜在漏洞并按优先级排序，并可通过与 WAF、API 网关、SIEM、ITSM、工作流工具或其他服务相集成，来以手动、半自动或全自动方式执行修复操作。除此之外，考虑到客户的技术堆栈在快速扩展，客户还审视了多种集成。