Akamai 客户案例

利用 Akamai API Security 保护客户安全

安全领导者帮助数千名客户保持合规，
同时保护数千个 API 的安全

Netskope 是一家全球网络安全领导者，正在重塑其云、数据和网络安全架构。数千家客户（包括财富 100 强企业中超过 25 家）要依靠 Netskope 应对不断变化的威胁，促进技术转型，并帮助他们遵守监管规定。

在 Netskope 提供保护的诸多任务关键型技术领域中，其中一个就是要负责保护全球数以万计的 API。该公司意识到，只有跳出传统应用程序安全防护的圈子，采用新方法才能完成这一艰巨任务。了解到客户的 API 安全态势存在漏洞后，Netskope 向 Noname Security（现已被 Akamai 收购）寻求用于保护客户免受 API 恶意攻击所需的下一代工具。

超越防火墙

无论客户是部署小型应用程序还是部署包含大量微服务的大型应用程序，他们实际上都在使用 API，这意味着每一个暴露的 API 都是攻击面的一部分。例如，Netskope 发现，客户的 API 资产中存在未检测到且 Netskope 也未察觉到的滥用行为。因此，Netskope 的 AppSec 团队开始寻找一种解决方案，既能保护他们自己的 API，也能保护其客户的 API，以及其他面向公众的数字资产。

Netskope 知道这个问题并非传统问题，这意味着他们无法使用 Web 应用程序防火墙一类的传统解决方案，也无法进行传统的应用程序安全测试。考虑到日志数量、发现的攻击类型以及 API 滥用类型，Netskope 需要采取不同的方法解决问题。

位置

美国加利福尼亚州
圣克拉拉
netskope.com

行业

高科技

解决方案

Akamai API Security

重要影响

- 全面保护 API 整个生命周期
- 实时阻止 API 攻击
- 自动创建 API 规范

Netskope 的代理 CISO James Robinson 也明白，尝试在整个企业范围进行扩展时，他的团队需要利用机器学习和先进工具来全面监测其 API 资产。安全团队很清楚，他们需要与开发人员通力合作才能上新一款工具。

安全团队的胜利

Netskope 决定使用 Noname API Security Platform（现为 Akamai API Security 的一部分）在预生产和生产过程中保护其 API。为确保生产过程中 API 的安全，他们利用 Akamai API Security 中的“发现”模块，掌握了客户的内部、外部和第三方 API 的准确清单，并对流经这些 API 的所有敏感数据进行了分类。掌握准确清单后，他们接着使用了“运行时保护”模块实时检测异常和阻止 API 攻击。

从预生产角度来看，Netskope 利用了 Akamai 的 API 安全测试解决方案来帮助企业在部署 API 之前先对 API 进行测试，以查找漏洞和错误配置。该解决方案可以自动运行 100 多个模拟恶意流量的动态测试，这不仅有助于企业开发人员保护其代码，还可以确保他们即将面向客户发布的 API 产品的安全。

在评估阶段，开发人员立即发现了可以让自己的工作生活更加轻松的功能。他们发现，当某个 API 规范已经过时，没有可用的规范时，Akamai 可以帮助开发人员快速构建一个规范。他们不必通过查看代码来理解 API，因为 Akamai 会自动为他们创建规范。对于日志和事务也是如此。开发人员可以在不同系统中进行查询，也可以查看日志行。

毫不意外地，选择这个平台也成为安全团队的重要成功决策。该团队不仅开始检测传统攻击，还能发现更复杂的威胁。

> 在内部，当我们开始探索该解决方案时，我们肯定需要与开发人员展开合作。没有他们的支持，你就无法进入他们的关键系统，总的来说就是他们应用程序的核心。
>
> —— James Robinson
> Netskope 代理 CISO

展望未来：让客户保持合规

未来，Netskope 计划通过 Akamai 解决 API 管理问题，确保自身及其客户遵守全球不断增加的数据隐私法律和规定。此外，在云端和本地部署了 Akamai API Security 后，他们还计划继续探索其他应用场景。对于他们自身以及该企业在公共部门和其他高度监管行业的客户来说，本地部署已经带来了巨大变革。

> Noname 不仅是赢家，而且更为重要的是，他们还支持更出色、更快速的部署，从而让我们更快进入市场。
>
> —— James Robinson
> Netskope 代理 CISO

企业正在迅速采用安全访问服务边缘 (SASE) 架构，以随时随地保护移动中的数据，为数字化转型工作提供支持，并通过技术实现更高的效率和投资回报率 (ROI)。Netskope 在 CASB、SWG、ZTNA、防火墙即服务以及安全服务边缘 (SSE) 的其他组件方面已经成为公认的专家和创新者，其中 SSE 描述了成功的 SASE 架构所需的安全服务。

然而，尽管 SASE 很受欢迎，但供应商信息难以理解，通常还会出现让人质疑是否为“SASE”的各种零散产品。大多数此类产品既非本机集成，也无法简化技术环境，而且还缺乏关键的网络和基础架构转型功能，所有这些都会引发更高级别安全事件、网络停机和投资回报率低的风险。

在一个完全融合的 SASE 平台中组合运用 Netskope Borderless SD-WAN 与 Netskope Intelligent SSE，这以另辟蹊径的方式解决了这些挑战。