AKAMAI 产品简介

API Security

Akamai API Security 是一款保护您的 API 免遭业务逻辑滥用和数据窃取的智能化解决方案

API 威胁在不断演变

API 每天都在推动您的业务发展，将您的业务与合作伙伴、供应商和客户紧密相连。然而，每个 API 同时也会增加您的攻击面，而攻击者深知这一点。API 攻击正在快速增多并不断演变，而且攻击的方式通常不会被 Web 应用程序和 API 保护措施察觉。如果缺乏一份全面的 API 清单，您的团队将面临监控盲点，并且您企业的 API 安全也无法得到有效保障。

为什么选择 Akamai API Security？

我们的平台可在 API 的整个生命周期为其提供保护，覆盖从开发到生产的各个环节。API Security 专门面向将 API 暴露给合作伙伴、供应商和用户的企业而构建，它可以发现您的 API、了解其风险态势、分析其行为，并阻止内部潜伏的威胁。

API Security 的关键功能

发现

企业存在未被发现的 API 这种情况很常见。然而，没有准确的 API 清单，您的企业将面临诸多安全风险。别再盲目猜测了，让我们来助您一臂之力：

- 无论配置或类型如何（包括 RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC 和 gRPC），该产品均可找到并列出所有的 API
- 检测休眠、遗留和僵尸 API
- 识别被遗忘、被忽视或未知的影子域名
- 消除监控盲点，发现潜在攻击路径

测试

当前应用程序开发的速度非常快，达到了前所未有的水平。这也意味着安全漏洞或设计缺陷更容易被忽视。利用我们的 API Security 测试套件，您可以：

- 自动运行 150 多个模拟恶意流量（包括 OWASP 十大 API 安全威胁）的测试
- 在 API 进入生产环境之前及时发现漏洞，从而降低攻击得逞的风险
- 依据已确立的管理策略和规则，对 API 规范进行检查
- 根据实际需求或在 CI/CD 管道中运行以 API 为重点的安全性测试

对企业的好处

发现
了解您的 API 攻击面。降低 API 清单和文档更新的成本。改善遵从法规要求和内部政策。

测试
通过及早发现问题，减少补救成本。在不牺牲开发速度的同时，提升代码质量。通过加快产品上市速度，增加收入。

检测
通过准确了解发生的事情，获取重要的业务情境信息。推断问题产生的原因，并揭示可能带来的影响。确定应采取何种措施来进行补救。

响应
通过立即阻止攻击来降低风险。及时修复漏洞以避免其被攻击者利用，从而降低成本。减少因停机造成的收入损失。

检测

简单的 API 配置错误就可能使您在网络犯罪分子面前毫无防御能力。一旦黑客入侵，他们便能快速访问并泄露您的敏感数据。使用我们的平台，您可以：

- 自动扫描基础架构，从而发现配置错误和隐藏的风险
- 创建自定义工作流，从而通知主要利益相关者有关漏洞的情况
- 确定哪些 API 和内部用户能够访问敏感数据
- 为检测到的问题分配严重程度评级，从而确定补救工作的优先级

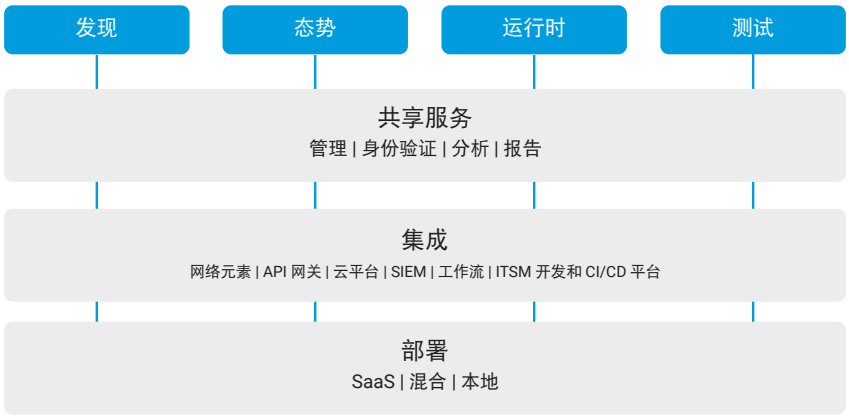
响应

如今不再是您的企业是否会遭受攻击的问题，而是何时会遭受攻击的问题。因此，您必须具备实时检测和阻止攻击的能力。使用我们基于人工智能 / 机器学习的异常检测系统，您可以：

- 监控数据篡改和泄漏、策略违反情况、可疑行为以及 API 攻击
- 无需进行额外的网络调整或安装难以部署的代理，即可轻松分析 API 流量
- 与现有工作流（票务、安全信息和事件管理 [SIEM] 等）集成，从而向安全 / 运营团队发出告警
- 通过部分或全自动化补救，实时防止各类攻击和滥用行为

Akamai 的独特之处：在边缘拦截

Akamai App & API Protector 可以发现并抵御通过 Akamai Connected Cloud 运行的应用程序和 API 所面临的 API 威胁，并可以阻止包含 API Security 发现的存在潜在威胁的任何流量。在联合部署的情况下，Akamai 的 API 防护措施可对 API 提供全面、持续的监测，让您能够发现、审计、检测和应对全部应用程序资产中的 API 安全问题。



想了解 API Security 的工作原理吗？请访问 akamai.com/apisecurity，和我们的团队安排一个合适的时间进行交流。

扫码关注，获取最新CDN前沿资讯