Akamai

API 安全态势管理权威指南

目录

为什么保护 API 安全已成为当务之急

在速度至关重要的行业，企业的开发人员利用 API 可以高效地构建工具或产品。API 不仅方便开发人员使用，还是实现软件与数据资产互操作的关键，但是，API 的安全防护没有跟上创新的步伐。

84% 的企业在过去 12 个月里遇到过 API 安全事件，较 2023 年 78% 的比例有所增加。[1] 导致此情况的部分原因在于，API 也能够提高攻击者的效率。很多 API 在构建时存在错误配置、代码编写错误和缺少身份验证控制等问题。因此，攻击者轻而易举就能实施 API 攻击，并且利用这种方式直接窃取数据。

在数据方面，只有 27% 的企业掌握了完整的 API 清单，并知道哪些 API 会返回从客户数据到知识产权的敏感数据。该比例较 2023 年 40% 的水平有所下降。[2] 随着攻击数量的增加以及监测能力的下降，企业需要一种方法来评估和增强其 API 安全态势。

1 和 2 的来源：Akamai，2024 年度 API 安全影响研究

什么是全面的 API 安全防护

随着您的企业越来越多地使用 API，攻击面也会相应扩大，产生新的安全挑战。

在保护 API 安全方面，企业传统上使用的工具（例如，API 网关和 Web 应用程序防火墙）都可以提供一定程度的保护。但是，API 资产变得越来越复杂，例如包含大量难以查看且难以保护的不受管 API，做出改变已是势在必行。

API 在企业的安全策略计划中占有重要地位。而专业的 API 安全防护解决方案旨在应对当今 API 风险和攻击方法，它可以为上述计划的执行提供必要的监测能力和各种功能。它与纵深防御的概念并无二致，在纵深防御中，各种工具相辅相成以覆盖攻击路径的每一步。

全面的 API 安全防护平台旨在提供 API 发现、态势管理、运行时保护和安全测试等功能，它可以帮助您发现隐藏的 API 风险、识别 API 攻击路径并实时抵御您未发现的威胁。

在我们发布的另一份与 API 有关的电子书《API 发现权威指南》中，我们探讨了 API 安全防护的第一关键要素——找到您的 API。在您发现贵企业使用的所有 API 并将它们加入清单之后，下一步便是增强整体 API 安全态势。

对于购买了第三方提供商的应用程序，并且将其作为自己的应用程序进行使用、品牌化和销售的公司来说，态势管理尤为重要。举个例子，近五年生产的新车几乎都带有如出一辙的远程信息处理功能。如果攻击者在某个制造商的 API 端点内发现了漏洞，他们便可以轻而易举地获得入口点，进而发起远程帐户接管攻击和实施数据入侵。

本指南涵盖的内容

API 态势管理为您提供了在 API 的整个生命周期内管理、监控和维护 API 安全所需的工具。本权威指南聚焦 API 安全态势管理的关键要求，包括漏洞检测和敏感数据保护。文中将探讨态势管理的方法，并介绍 Akamai API Security 解决方案的态势管理功能。

为什么需要进行态势管理？

API 态势管理可确保您在API 安全防护方面全力以赴。它可以发现传输的数据类型、是否存在任何漏洞或错误配置，以及 API 是否经过了正确的身份验证等，从而有助于您了解所发现的 API 存在的风险。它能够识别并快速修复 API 漏洞，让您可以提前采取纠正措施，防患于未然。

全面的态势管理让您可以监测与 API 有关的所有活动，这样您便能够实施安全策略、确保遵守法规并审查 API 生态系统的变化。它可以保护您的 API 免受恶意攻击、未经授权的用户和数据泄露等威胁的影响，其中任何一项威胁都可能导致严重的声誉损失、业务损失和监管处罚。

只有 27% 的企业掌握了完整的 API 清单并知道哪些 API 会返回敏感数据，较 2023 年 40% 的比例有所下降。[3]

3. Akamai，2024 年度 API 安全影响研究

实施态势管理最佳实践可最大限度地减小 API 攻击面并抵御大多数 API 风险。要想实现良好的态势管理，为您的企业建立完整的 API 和敏感数据存储清单至关重要。在下一页中，我们将讨论 API 态势管理的其他要素：漏洞检测、API 监控和问题修复。

- ## 漏洞检测

  分析：检查源代码是否存在常见漏洞、了解 API 与外部系统的交互方式以及评估 API 的授权和身份验证功能。

  观察：检查进出 API 的流量以识别错误配置、检测漏洞并了解 API 基准行为。

态势管理只是完整的 API 安全防护计划的其中一个要素，实施全面的生产前测试来防止漏洞进入生产环境同样重要。

- ## API 监控

  识别和监控生产环境中的 API 调用、跟踪 API 请求、检测与基准使用情况的偏差，以及在 API 用量超过预定义阈值时发出告警。

- ## 修复

  通过更改代码、微调安全设置或修补 API 缺陷来修复已发现的弱点或漏洞，提升 API 的安全性和合规性。良好的态势管理能够在漏洞遭到利用之前实施修复。

不可或缺的态势管理功能

您可能已经知道或者高度怀疑自己的 API 安全态势并未达到应有的水平。以下是您的态势管理工具必须提供的一些关键功能。

- **敏感数据分类**
  与传输信用卡信息的 API 相比，根据公共来源提供天气数据的 API 的敏感度要低的多。API 态势管理工具应该能够快速识别有多少 API 可以访问信用卡数据、电话号码、社会保障号 (SSN) 和其他敏感数据，以及已通过您的 API 访问敏感数据的用户数。

- **配置评估**
  用于代理和保护 API 流量的网络、API 网关或防火墙出现一处简单的错误配置，就可能给网络攻击带来可乘之机。
  强大的态势管理需要能够定期扫描基础架构和软件配置，包括日志文件和配置文件。定期扫描可帮助发现配置错误和漏洞并识别配置漂移带来的风险。

- **攻击者信心得分**
  寻找一个攻击者信心评分引擎，该引擎使用经过训练的先进机器学习算法来评估外部和内部信号，包括 API 行为、网络流量模式、地理位置数据、威胁情报源和其他背景因素。这可以帮助您确定检测到的运行时事件由恶意活动所导致的置信度。借助该独特功能，客户能够快速锁定关键威胁，并针对高概率攻击创建自动修复和通知流程。

- **自定义工作流**
  除了可自定义的严重性之外，您还需要能够创建工作流，以便在发现漏洞时立即采取行动。自定义工作流可能包括创建故障单、通知关键利益相关者以及更新网络配置。

- **自动生成的文档**
  API 文档会告诉 API 使用者 API 的功能及使用方法。您必须根据规范对安全的 API 进行合规性评估并准确记录。文档不完善或没有文档会导致安全测试难以完成，这使得进入生产环境中的 API 可能包含未发现的漏洞，导致风险上升。

而 API 开发的外包往往会使此问题变得更加严重。无论问题的根源是什么，如果您想让自己的 API 安全计划取得成功，那么文档过时、不完整和缺失都是不可接受的。

OpenAPI 规范（以前称为 Swagger 规范）定义了标准的接口说明。态势管理工具应该能够根据 API 的当前和未来状态自动生成完善的 OpenAPI 文档，以帮助确保所有 API 都得到了妥善记录并且文档包含的是最新信息。

保险业领军企业携手 Akamai 增强 API 安全态势

随着消费者从实体店转向线上，金融服务公司必须加快创新步伐。与很多同行一样，美国优秀的补充医疗保险提供商 Aflac 也面临着日益严峻的 API 安全挑战。

Aflac 转为使用 Noname API Security Platform（现为 Akamai API Security 的组成部分）来满足自身需求。其安全团队利用态势管理模块识别流过公司 API 的数据类型，从而监测哪些 API 访问了敏感数据并识别数据访问中的所有异常情况。

有关更多信息，请阅读完整的 Aflac 案例研究。

> “我们知道，我们的 API 使用量非常大，所以希望能够确保了解每个 API 的用途，能够完全地监测 API 的运行情况，以及能够持续测试安全风险。
>
> —— Aflac 公司安全运营和威胁管理副总裁 DJ Goldsworthy

Akamai 的态势管理方法

Akamai API Security 解决方案的态势管理模块让您可以全面了解流量、代码和配置，以评估贵企业的 API 安全态势。Akamai 可确定 API 和 Web 应用程序的真实攻击面，并发现通过您的 API 移动的所有敏感数据形式，帮助您保护敏感数据的安全。

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。一旦黑客入侵成功，他们便能快速访问并泄露您的敏感数据。

Akamai API Security 解决方案的态势管理模块提供以下关键功能：

- 带外集成，用于本地以及混合云和公有云中的持续 API 发现
- 简单、可搜索的 API 清单，提供架构、网络布局和数据类型的详细信息
- 自动 API 文档生成 (OAS/Swagger)
- 对 API 错误配置和漏洞进行情境感知分析并确定优先级
- 检测 OWASP 十大 API 安全漏洞中的所有漏洞
- 自动发现敏感数据和 API 变化并进行分类

API 暴露

除了发现 API 代码内的风险之外，观察 API 流量并关注典型与非典型的行为以及观察和关注网络环境中的情况也很重要。

Akamai API Security 解决方案的态势管理会尽可能查看更广泛的来源以检测漏洞，包括日志文件、历史流量回放、配置文件等。该解决方案会检测 OWASP 十大 API 安全漏洞中的所有漏洞，并保护 API 免受数据泄露、授权问题、滥用、不当使用和数据损坏的影响。

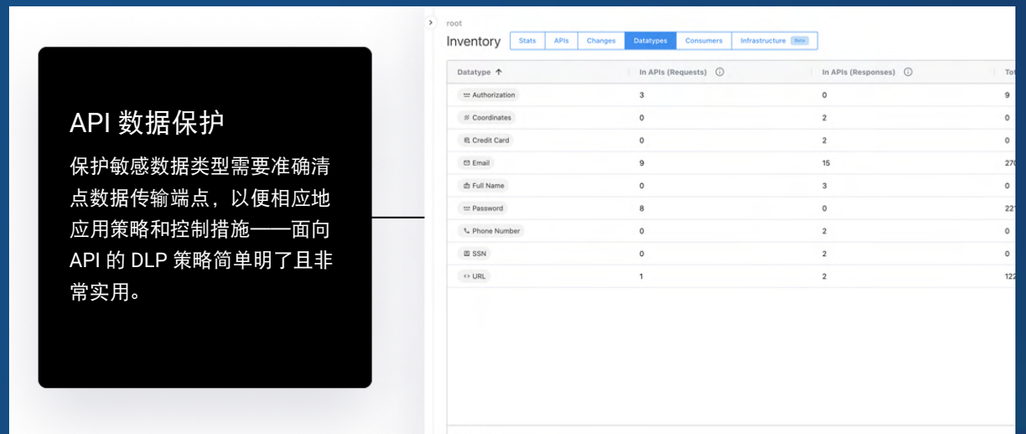
Akamai 可以智能地识别潜在的漏洞并划分优先级。通过集成到 WAF、API 网关、SIEM 和 ITSM 工具、工作流工具及其他服务中，该解决方案能够以手动、半自动或全自动方式修复漏洞。

API 数据保护

保护敏感数据类型需要准确清点数据传输端点，以便相应地应用策略和控制措施——面向 API 的 DLP 策略简单明了且非常实用。

随着 API 使用的增加，合规性呈现出了一个全新的维度。一系列法规纷纷出台，以应对日益扩大的攻击面。受监管的行业现在必须将 API 纳入其合规计划中。

Akamai API Security 解决方案的态势管理模块可识别流过您的 API 的所有敏感数据形式，包括所有个人身份信息 (PII)，例如信用卡数据、SSN、地址、保险信息等。通过减少对这些数据类型的访问并实施数据管理框架，我们可帮助您确保敏感数据位于所需的位置并保护其免受恶意威胁的侵扰。



API 态势管理如何为您提供助力

每当有客户、合作伙伴或供应商与贵企业进行数字互动时，后台都会有相应的 API 来帮助实现数据（通常是敏感数据）的快速交换。监测整个企业中的每个 API 并评估其风险属性（例如，哪些 API 会返回敏感数据），能够帮助您保护贵企业免受快速增加的攻击媒介的影响。API 安全态势管理还可以帮助您确保遵守旨在防止数据泄露的全球法规。

了解要求对所有 API 进行监管和保护的数据保护法规。

预约定制化 Akamai API Security 演示，了解我们如何为您提供帮助。

扫码关注 - 获取最新云计算、云安全与 CDN 前沿资讯

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 **akamai.com** 和 **akamai.com/blog**，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 12 月。

Akamai