Akamai

白皮书

向 API 安全防护解决方案供应商询问的 13 个问题

前言

当下，企业对企业的 API 网络呈指数级增长。不断壮大的物联网设备阵营也给开发人员带来了新契机，让他们可以借助 API 将真实数据融入到应用程序中。

然而，API 在为企业创造众多的创新和增长新机会的同时，也不可避免地带来一系列新的安全挑战，其中包括：

- API 凭据被盗用
- 未被察觉的 API 侦察
- 配置不当的身份验证和授权
- 未加保护的影子 API 和僵尸 API
- 远程代码执行、注入、本地文件包含以及其他攻击手段
- 数据泄漏或外泄
- API 抓取
- 业务逻辑滥用

安全解决方案供应商为企业提供了诸多方案来检测和抵御各种 API 威胁，但是这些方案并不都是高效且易于使用的。

在与 API 安全防护解决方案供应商进行讨论时，您可以提出以下 13 个问题，以评估供应商的产品是否能有效满足贵公司的 API 安全防护需求。

1 你们的 API 安全防护产品能否在企业范围内执行 API 发现？

在安全团队所面临的重大挑战中，缺乏全面、准确的 API 清单是其中的一项，这导致他们无法了解企业所暴露的 API。许多未被记录的影子 API（即那些被安全团队忽略的 API）并未被纳入到正式的 API 管理和安全框架中。僵尸 API 也很常见，在企业的印象当中，这些 API 已经退役，但实际上它们依然可以访问。即使在已经获得认可并且有记录的 API 中，也可能存在未被记录的 API 参数，这给攻击者提供了可乘之机。因此，发现所有南北向、东西向和出站 API 是非常必要的。为了确保在企业范围内实现全面的 API 监测，只有一个有效的方法：对来自所有技术和云平台的现有 API 活动数据进行检查。

2 你们的产品能否持续地发现 API？如果可以，这个流程需要人工参与的程度如何？

随着 DevOps 的快速发展，不断有新的 API 涌现，也不断有 API 消失。因此，某个特定时间点的 API 清单往往是不完整的。为了确保新记录的 API 能够被及时加入到清单中，并对其进行分析和保护，您的 API 安全防护产品必须具备持续发现 API 的能力。此外，它还应该具备检测未来可能出现的任何影子 API 或僵尸 API 实例的能力。此外，有些产品会给您的安全团队带来持续的负担，使得他们难以理解并解释所发现的结果，并据此采取相应的行动，此类产品将不具可持续性。相比之下，一些产品利用自动化和机器学习技术来发现和评估 API，它们不会给安全团队的日常任务列表增加更多人工任务，只有这样的产品才能让贵公司更加顺利地运营。

3 你们的产品能对我们的 API 文档工具和流程提供哪些帮助？

将文档记录方法集成到 API 安全防护平台中会带来诸多好处，因此我们建议您向供应商核实其是否具备这方面的能力。例如，在持续集成/持续交付 (CI/CD) 流程中，自动将现有的 Swagger 文档上传到您的 API 安全防护平台，这将有助于提高影子 API 检测和影子参数识别的准确度（假设供应商具备将发现的 API 参数与已记录的参数进行比较的能力）。此外，对于任何缺乏文档记录的 API，您的安全防护平台应具备一键式创建自定义 Swagger 文件的功能，这将有助于开发人员启动并优化文档记录流程。

4 在我们的环境中部署你们的产品需要投入多少时间和工作量?

要开始建立此类防护机制，最有效、最快捷的方法便是使用基于安全即服务 (SaaS) 的 API 安全防护产品，因为它们会采用非侵入式方法收集和分析来自现有系统的 API 活动数据。只需要几分钟，您就可以将精心设计的 SaaS API 安全架构集成到自己的环境内，从而更快创造价值并消除与系统更新相关的持续成本和风险。如需进一步提高敏捷性，可以找一个能同时提供 Web 应用程序和 API 保护 (WAAP) 以及 API 检测和响应的供应商，以便 API 流量数据可以在入站流量保护解决方案与企业内所有 API 流量保护解决方案之间无缝流动。

5 你们的产品如何帮助我们识别有风险的 API，并确定这些有风险 API 的优先级?

第一次查看全面的 API 清单时，既会感到充满力量，也会感到压力巨大。许多安全团队都感到信息量过大，难以确定应该将 API 安全防护工作的重点放在哪里。为了避免这种情况的发生，最好是选择一个能够为您完成这些工作的 API 安全防护产品，具体包括以下工作:

- 突出显示存在允许访问敏感数据的 API
- 按类型自动标记敏感数据（例如个人身份信息、电子邮件地址、信用卡数据等）

除此之外，您的 API 安全平台还应该允许您创建自定义的标签类别，以便 API 团队和安全团队使用符合业务目标和安全考量的通用语言。

6 你们的产品是通过行为分析来确定预期行为的基准并发现异常的吗?

许多类型的攻击都是通过攻击签名检测到的，并在 WAAP 级别加以阻止。然而，在开放式 Web 应用程序安全项目 (OWASP) 发布的 2023 年 API 安全十大漏洞列表中，发现了许多无法通过上述方法发现的攻击类型（例如遭到破坏的对象级授权）。这类攻击更为被动且以业务滥用为主，因此更难以检测到。要有效抵御所有类型的 API 威胁媒介，唯一的办法就是使用行为分析和机器学习技术。要进行真正的行为分析，需要大量的数据集，并利用相应的机器学习算法来学习您的独特环境，同时还需要具备足够的灵活性和敏捷性，以便根据全球信息自动更新和调整。SaaS 模型就是唯一能够高效地完成这些活动的有效方法。

7 你们的产品能否收集并分析包含足够信息量的重要数据集，从而有效地确定正常行为的基准并检测出异常吗?

许多 API 安全防护产品都专注于监控个别的 API 调用，或者充其量只监控短期会话活动。这显然是不够的，因为许多合法的业务流程以及许多的攻击都会经历一个比较漫长的过程。在分析 API 使用情况时必须经历一个演变的过程（至少 30 天）。这样才能更全面、更准确地确定预期行为的基准，包括每个月仅有一次的业务流程（如开票等）。另外，也只有这样才能检测到在数天或数周的时间内通过大量 API 会话缓慢实施的攻击。

8 你们的产品能否逐一识别出原始 API 数据中的所有实体、关系和活动，以便为我们提供业务情境?

要让 API 活动数据更具有实际参考价值，最好的办法是用具有业务含义的 API 使用情况情境数据来充实它。下面的识别和标记功能对于 API 安全防护平台评估和分析不同实体间的关系至关重要：

- API 用户（用户实体）的表示，如 IP 地址、API 密钥、访问令牌、userID、partnerID、merchantID、supplierID 等
- 业务流程（业务流程实体）的表示，如预订、支付、开票、帐户余额等

只有在此级别进行精细分析，才能将 API 生成的海量数据转化为有意义、易于理解的预期行为基准。

9 你们的产品能否在时间线上绘制 API 实体与活动的关系图，从而展示行为随时间的变化？

在宏观上了解和监控 API 活动及威胁固然重要，但将分析重点缩小到特定实体上的能力同样关键。例如，当发现特定业务伙伴存在异常行为时，能够在时间线上查看该实体的所有活动，这一能力就变得十分重要。对业务流程实体也同样如此。在时间线上查看 API 内的每个实体都发生了什么以及何时发生的，这是一种非常强大的可视化功能，可以让 API 的正常使用和业务滥用情形一目了然。另一个强大的工具是回顾活动以查看生成告警前后发生情况的能力，它可以帮助您深入了解业务逻辑滥用的具体情况。

10 如何将你们的产品集成到我们现有的工具、流程和工作流当中？

向您的安全信息与事件管理 (SIEM) 产品发送告警确实十分有用，但这仅仅是个开始而已。在检测到安全威胁和事件时，越来越多的安全团队开始使用更精密的安全编排、自动化和响应 (SOAR) 工具来启动预定义的工作流。而且，许多 API 安全防护问题需要由安全团队以外的开发人员来解决，所以您的 API 安全防护平台还需要与开发团队的问题跟踪与工作流管理工具集成。当您的安全防护工具在分析 API 流量时，它还应该能够使用 API 来协助编排 CDN、Web 应用程序防火墙或 API 网关的响应，并允许您创建自己的响应行动手册。

11 我可以查询你们产品的 API 和活动数据，以便主动搜寻威胁和抵御风险吗？

安全和开发工具的集成不能仅仅是将单向告警发送到您工具中的黑盒。您的安全团队和 API 团队需要的是挖掘告警或问题背后的源数据的能力。所以，您需要寻找的是允许用户通过内置 Web 界面或 API 来查询 API 详细信息的 API 安全防护平台，这样才能将该平台与其他首选的工具和界面相集成。它还将赋能您的安全团队，使他们能够高效、主动地执行威胁搜寻。另外，它还可以帮助开发人员和其他非安全领域的相关人员了解攻击者是如何合法利用 API 来发起攻击的。

12 你们会采取哪些措施来确保所收集的有关我们公司的敏感数据受到保护?

在当今的威胁格局下，要想通过高级行为分析来保护 API 的安全，只有在云的量级下才有可能实现。考虑到 API 数据集的规模和敏感度，您必须要求安全解决方案供应商确保对您的数据进行保护。此外，检查供应商用于保护其云基础架构的措施固然重要，但这只是第一步。您应当要求您的 API 安全防护解决方案供应商采用令牌化等先进技术。令牌化是一种将敏感数据替换为匿名化令牌，然后再将它们传输到云端。通过这种方式可以确保数据隐私安全，即使供应商或其上游云服务提供商遇到安全事件，也能确保数据安全无虞。

13 你们的解决方案可以让我们更精细地访问 API 活动数据吗?

在合规性以及攻击防范等所有领域中，数据是至关重要的战略元素。许多供应商会提供一段时间内存储的 API 数据，但您必须深入了解他们所提供的内容。仅提供告警的解决方案无法展现事件的全貌，因为被入侵的 API 活动是随着时间的推移缓慢进行的，而并非在发出告警后立即发生。而提供全面解决方案的供应商会记录所有 API 活动，帮助您消除盲点，并提供工具来详细审视该活动，而不是将其交给模糊的机器学习模型而不管不顾。由此可见，这种精细访问数据的能力至关重要，它使您能够主动监控威胁，而不是在收到攻击告警后才意识到问题的存在。

向 API 安全防护解决方案供应商询问的 13 个问题

1. 你们的 API 安全防护产品能否在企业范围内执行 API 发现?
2. 你们的产品能否持续地发现 API? 如果可以，这个流程需要人工参与的程度如何?
3. 你们的产品能对我们的 API 文档工具和流程提供哪些帮助?
4. 在我们的环境中部署你们的产品需要投入多少时间和工作量?
5. 你们的产品如何帮助我们识别有风险的 API，并确定这些有风险 API 的优先级?
6. 你们的产品是通过行为分析来确定预期行为的基准并发现异常的吗?
7. 你们的产品能否收集并分析包含足够信息量的重要数据集，从而有效地确定正常行为的基准并检测出异常吗?
8. 你们的产品能否逐一识别出原始 API 数据中的所有实体、关系和活动，以便为我们提供业务情境?
9. 你们的产品能否在时间线上绘制 API 实体与活动的关系图，从而展示行为随时间的变化?
10. 如何将你们的产品集成到我们现有的工具、流程和工作流当中?
11. 我可以查询你们产品的 API 和活动数据，以便主动搜寻威胁和抵御风险吗?
12. 你们会采取哪些措施来确保所收集的有关我们公司的敏感数据受到保护?
13. 你们的解决方案可以让我们更精细地访问 API 活动数据吗?

正如您可能已经意识到，Akamai API Security 能够有效为您提供上述列表中推荐的所有保护。探索我们的解决方案。