API 安全解决方案买家指南

加强部署以迎接 API 安全挑战

当今企业纷纷迈向以云为中心的架构，数字化程度越来越高，其 API 的使用范围和规模不断扩大，价值也随之增加。现在，API：

- 运行在应用程序与服务的核心位置，向您的客户和合作伙伴提供服务，包括最新的 AI 创新
- 嵌入整个云环境中，无论是在开发人员使用的服务中，还是在工程师处理的工作负载中，都能发现它们的身影
- 本身即代表着收入来源，可帮助您发展业务并构建开发人员生态系统

不过，有 78% 的 IT 和安全专业人员遇到过 API 安全事件[1]，如果您也遇到了，那么相信您对 API 风险与日俱增的问题已有亲身体会。API 暴露在外或错误配置的情况很普遍，这些 API 没有得到妥善保护，很容易受到攻击。甚至于很多企业往往都没有摸清他们的所有 API，导致这些 API 处于不受管理的境地。这些休眠（或者僵尸）API 成为了主要的攻击媒介。

随之而来的风险很高。对 API 的攻击会损害企业的收入、恢复能力以及法规合规性。很多企业尚未采取适当的控制措施和功能来防范 API 攻击。诚然，很多公司现有的堆栈中会有一些 API 工具，包括 API 网关和 Web 应用程序防火墙。尽管这些工具具备一定的防护能力，但它们并非设计用来提供充分的监测功能、实时安全性和持续测试功能，无法抵御现代化 API 攻击。

1. Akamai Technologies, “API Security Disconnect Report,” 2023

那么，如何才能全面保护您的 API 资产？虽然过去几年中涌现出了很多 API 安全产品，但随着供应商的范围及其功能不断扩展，想要充分了解这些信息变得比较困难。

应对如今的威胁需要全面的 API 安全解决方案，涵盖四个关键领域：API 发现、态势管理、威胁检测和修复以及安全测试。本买家指南介绍了全面 API 安全解决方案所应具备的关键功能，如何针对开发和维护安全的 API 定义所需的功能及安全控制措施，以及如何找到并保护您生态系统中的每个 API。

全面 API 安全解决方案的关键功能

要确定所需的 API 安全功能，您必须要了解面对的安全挑战的性质。

API 通常散布多个环境中，囊括了从本地到混合云的各种环境。而且您的 API 生态系统很可能远远超出了您自己的网络和云环境范围，这进一步加剧了复杂性。想象一下您的 API 已与属于第三方的应用程序、服务及系统建立无数连接，而这些第三方是否重视 API 安全性无从确定。

此外，以下信息也难于实时了解：

- 您的 API 被路由到何处
- 它们的配置方式
- 它们传输了哪些敏感数据
- 它们带来了哪些风险

随着企业在匆忙地开发和推出新的应用程序和 API，攻击面呈指数级扩大。您的企业可能有大量老旧的 API，它们是多年前构建的，当时 API 安全还不是一项关键需求。

缺乏监测能力导致了令人担忧的结果：只有四成的安全专业人员掌握了完整的 API 清单，并知道哪些 API 在调用时会返回敏感数据。其中很多 API 调用都源自恶意攻击者，用于测试是否存在漏洞，而一旦发现漏洞后，随之而来的攻击往往无休无止。

在审查声称能够全面保护 API 的安全供应商时，您需要确保他们在四个关键领域都拥有成熟、已投入生产环境的控制措施和功能，这一点非常重要。

请继续阅读，了解可用于审查供应商能力的一系列买家检查清单。

01

API 发现

企业存在未被发现的 API 这种情况很常见。但是，如果没有准确的 API 清单，企业将面临各种风险。要有效地清点 API，您需要能够：

- ☑ 找到您的所有 API 并将其加入清单中，而无论配置或类型如何
- ☑ 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

02

API 态势管理

简单的 API 配置错误就会为攻击者敞开大门。一旦攻击者入侵成功，他们就能快速访问并泄露敏感数据。要了解您所有 API 的配置方式，您需要能够：

- ☑ 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

03

API 威胁检测和修复

API 攻击已经到了无法避免的地步。要想有效地检测和修复威胁，您需要能够：

- ☑ 监控数据篡改和泄露、策略违反情况、可疑行为以及 API 滥用
- ☑ 分析来自所有来源的 API 流量，并将分析功能集成到现有工作流（工单、安全信息和事件管理等）中，以便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

04

API 安全测试

对于开发人员构建的每个应用程序，速度都至关重要，但过于追求速度往往会让漏洞或设计缺陷更难以被检测到。要妥善地测试 API，您需要能够：

- ☑ 运行各种自动化测试，模拟恶意流量并遵循底层 API 业务逻辑
- ☑ 在 API 进入生产环境之前发现漏洞，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 为重点的安全测试

API 发现：深入了解关键功能

很多企业同时在运行遗留 API 和新 API。在生产环境中，存在运营团队或安全团队都不知道的不受管 API 很常见，但这会让企业面临一系列网络安全风险和运营难题。有多重因素可能会导致产生恶意 API，例如走捷径、进程故障和停用后未关闭等。在下一页中，我们将提供需要注意的关键示例。

商业 API

一些商业软件包会包含用于连接其他应用程序及外部数据源的 API。这些 API 可能会在无人注意的情况下被激活。

停用失败

一些 API 也可能已正式停用，但由于操作疏忽而仍在运行。这些 API 有时被称为僵尸 API。

旧 API 版本

有时，某个 API 的旧版本从未被停用。在软件更新期间，旧版本可能不得不与新版本共存一段时间。但如果负责停用 API 的人员从公司离职、被重新分配了工作或者干脆忘记了停用旧版本，会出现什么情况？

走捷径和进程故障

一些恶意 API 是未能告知正确人员的产物。例如，某个业务线 (LOB) 团队可能会创建用于满足特定需求的 API 而未告知 IT 部门，或者开发人员可能更关注执行而不是过程。因收购而“继承”的 API 也经常会被忽略。这些类型的恶意 API 往往被称为影子 API。

当您与供应商进行沟通时，请让他们说明如何确保能够识别并处理恶意、遗留、僵尸和影子 API，以防被利用。遗留和僵尸 API 通常是 API 安全中的薄弱环节。因此，至关重要的是发现不受 API 网关管理的 API 并找到它们，将它们加入清单，并确定需要修复还是停用它们。

关键的 API 发现功能

API 安全解决方案应包含以下发现功能

API 资产发现和详细清单

API 发现工具必须能够找到并识别您拥有的 API，而无论配置或类型如何，如 RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC 和 gRPC 等等。它还应该创建一个会自动更新以避免过时的清单，并提供根据任何属性搜索、标记、过滤、分配和导出 API 的功能。

检测休眠、遗留和僵尸 API

遗留和僵尸 API 可能出现在企业制定 API 安全计划之前。这些 API 通常没有人负责，并且会在没有被监测或采取安全控制措施的情况下运行。API 发现工具能够找到这些 API 非常关键。

影子域名发现

除了影子 API 之外，您可能还会有完整的影子域名，这是您对其一无所知的 API 域名。API 发现工具必须能够识别被遗忘、被忽视或可能构成安全风险的未知影子域名。

自动扫描

扫描是消除盲点并识别以下关键问题所必不可少的：

- 泄露的 API 密钥和凭据
- API 代码和架构暴露
- 基础架构配置错误
- 文档、GitHub 存储库、Postman 工作区等中的漏洞

确定这些和其他可利用漏洞来源的情报，同样有助于团队了解可能会被网络犯罪分子利用的潜在攻击路径。

限制定制开发

最后，有了适合的 API 发现工具，您应当不再需要针对流量来源进行定制开发工作。对于主要基础架构组件，这些工具应随预构建的集成提供。定制开发通常非常耗时，而且在源代码发生了更改时，可能需要重新设计集成，这对于时间上本就捉襟见肘的 IT 安全团队是不可取的。

API 态势管理：深入了解关键功能

由于各种趋势，例如从集中式 IT 转变为分散式 LOB 运营、云资源的使用增加以及向基于微服务架构的过渡，API 资产所面临的威胁正在迅速增加。

强大的发现功能（如上一节中所述）是保护您的 API 资产的第一步。您需要发现当前正在使用的所有类型的 API 并将它们加入清单。

为了管理所有 API 的安全态势，还有一些附加功能必不可少。您需要能够识别哪些 API 可以访问和传输敏感数据，并相应地对这些 API 进行分类——因为接触客户信息等数据的 API 肯定需要经过身份验证。此外，还必须识别会导致任何 API 更容易受到攻击的基础架构漏洞。

配置评估

很多网络攻击之所以得逞，是由于负责代理和保护 API 流量的网络、API 网关或防火墙中存在简单的配置错误。

API 安全解决方案应定期扫描基础架构和软件配置，包括日志文件、历史流量回放、配置文件等。这让您可以发现配置错误和漏洞，并消除配置偏移带来的风险。

可自定义严重性级别

当解决方案识别出环境中的新漏洞时，它还应该对已发现的问题分配一个严重性级别，以便确定这些问题的修复优先级。这些严重性级别应该可以根据企业的风险承受能力、监管要求和内部策略，对其进行自定义。

自定义工作流

除了可定制严重性等级之外，理想的态势管理工具还应该允许您创建自定义工作流，以便在识别漏洞后立即采取措施。这些工作流包括创建工单、通知主要利益相关者、更新网络配置等。

自动生成文档

API 文档可以向使用者说明 API 的作用及使用方法。各企业必须根据规范且准确的文档来评估安全 API 的合规性。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。

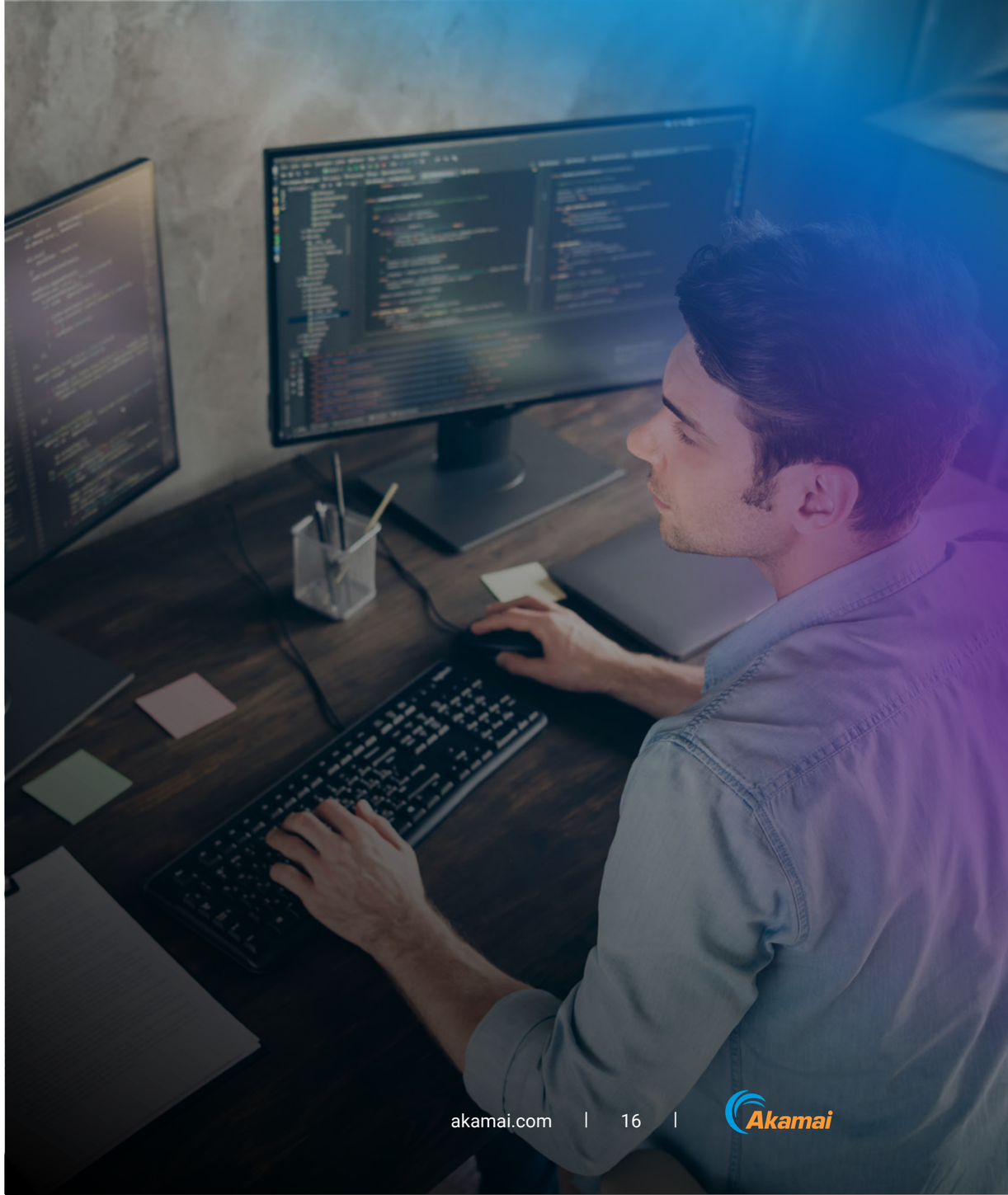
OpenAPI 规范定义了标准的接口说明。API 安全解决方案应该能够：

- 将 API 规范与实际可观察到的流量进行比较并找出差异，这让企业能够看到所部署的哪些 API 不符合规范并且可能存在风险。
- 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。确定这些和其他可利用漏洞来源的情报，同样有助于团队了解可能会被网络犯罪分子利用的潜在攻击路径。

API 威胁检测和修复：深入了解关键功能

尝试利用 API 漏洞进行攻击已是既定的事实。这不再是您的企业是否会受到攻击的问题，而是何时及如何受到攻击的问题。当务之急是迅速检测并阻止攻击，避免它们造成严重损害，例如泄露客户隐私数据。即使您已尽可能确保 API 的安全，但仍需要有效的运行时保护措施来检测数据泄露、数据篡改、数据策略违反情况、可疑行为和 API 安全攻击。这应该包括记录 API 流量、监控敏感数据访问、检测威胁以及屏蔽或修复攻击媒介。

在接下来的两页中，我们将介绍 API 安全解决方案应包含的关键功能。



实时带外监控

API 安全监控不得影响 API 流量或减慢其速度。寻找可以提供无代理方法的供应商，这样公司就能够加快部署速度并监测更多流量。而且，在适当的情况下（例如，复杂的本地环境中），解决方案还应该具备足够的灵活性来为代理提供支持。

API 安全解决方案应该对来自于已识别数据源的流量进行镜像，在后台对流量数据进行分析，并在发现任何问题后发出实时告警。

API 异常和漏洞利用检测

被动数据收集不足以满足要求，尤其是在 API 数量及 API 流量总量不断增加的情况下。解决方案必须持续分析 API 活动，以检测异常事件并向安全和运营团队发出告警。

高级工具包含 AI 和机器学习功能，可实时分析流量，并利用情境洞察来识别可能表示存在数据泄露、数据篡改、数据策略违反情况和其他 API 安全攻击的异常活动。

API 攻击防范

在识别异常或其他问题并生成告警后，时间便至关重要。解决方案必须检测通过 API 未经授权地移动敏感数据或者其他可疑的 API 滥用行为，并予以阻止。API 安全解决方案不仅应通过与现有防火墙和 API 网关的集成来阻止滥用，还应部分或完全实现修复自动化。半自动的修复措施应该可用于解决某些类型的告警。对于先前已识别但又重复出现的问题，您应该能够选择提供完全自动化的应对措施。

对攻击置信度进行评分

市场上的一些解决方案使用经过训练的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、地理位置数据和威胁情报源。通过使用此类情境因素，解决方案可以针对检测到的运行时事件，确定能够以多高的置信水平来确定事件是由恶意活动引发。

事件响应的集成

当事件发生时，API 安全解决方案必须包含必要的集成功能，以确保将修复任务分配给相应的团队。如果检测到配置错误、数据策略违反情况或可疑行为，那么应该将它们报告给 API 网关、SIEM 系统和其他信息安全引擎，以确保引起充分的注意。

一般来说，API 安全解决方案应该能够与企业使用的其他安全、监控和管理工具轻松集成。

API 安全测试：深入了解关键功能

很多开发团队都会犯的一个错误是，拖到太晚才开始进行 API 测试，从而导致测试成为了瓶颈。团队需要采取左移方法来确保在开发过程中尽早开始测试，以确保测试的全面性。有效的 API 安全测试能带来巨大的好处：

- **防止攻击**
  - 在 API 进入生产环境之前发现漏洞，您就可以降低攻击得逞的风险
- **改进合规性**
  - 全面测试将帮助您确保实现合规性，并避免遭受罚款和声誉受损
- **提升信心**
  - 严格有效的测试可以提升企业对 API 的信心，并帮助确保开发人员能够按时进行发布

市场上的一些供应商可以就如何修复环境中的问题以及如何启用全面 API 测试配置，向企业提供相关建议。这些建议可以包含用于配置正确身份验证或修复 API 依赖关系的操作步骤。相关好处如下：如果您可以解决环境内的业务逻辑问题，就可以增加针对测试进行优化的 API 的数量，从而扩大测试覆盖范围。

但是，API 安全测试的整体概念仍然有些模糊不清。开发团队可能并不完全了解它的含义。左移 API 测试过程分为三步：

1. **了解 API：**了解 API 的应用场景可以为测试提供信息，尤其是对于棘手的业务逻辑问题。
2. **确保您可以正确地与 API 进行交互：**确保您可以按预期使用 API。要验证您掌握的 API 的情况是否与 API 运作的方式相符，此步骤必不可少。
3. **向 API 发送攻击流量：**这可能包括手动操纵对 API 的请求、将模糊测试字符串插入请求中或者使用自动工具来执行 API 安全测试。正如现代化 IT 中的所有事物一样，自动化通常是在不牺牲速度的情况下大规模完成工作的最佳方式。

关键的 API 安全测试功能

API 安全测试应包含静态、动态和渗透测试。API 安全解决方案应包括相应的工具，用于促进全面测试并尽可能实现测试流程自动化。在 API 安全解决方案中寻找下列 API 测试功能：

主动的自动化 API 安全测试

自动化安全测试可以在 API 进入生产环境之前识别出配置错误、漏洞和不合规之处，从而显著降低风险和成本。

API 管理

仔细考虑角色、职责和策略等治理问题至关重要。这包括开发人员、安全工程师和平台工程师在执行层面的职责，以及策略监督和与风险相关的决策。API 安全解决方案应该让您可以依据已制定的治理策略和规则，对 API 规范进行检查。

CI/CD 管道和代码库集成

DevSecOps 是 DevOps 的一种变体，用于提升软件开发工作流的安全性。API 安全防护必须包含在 DevSecOps 计划中。API 安全解决方案应提供一套以 API 为重点的安全测试，这些测试可以根据实际需求运行或包含在 CI/CD 管道中运行。CI/CD 集成必不可少，因为它可以实现持续、快速的 API 安全测试，从而跟上应用程序开发的步伐。

综上所述：
识别和解决 API 安全漏洞

在数字化和以云为中心的程度越来越高的经济环境中，API 是企业服务客户、创造收入以及高效运营能力中必不可少的组成部分。但是，API 的持续增长、与敏感数据相伴以及缺少安全控制措施等因素，让 API 成为当今的攻击者眼中诱人的目标。

很多企业用于管理 API 和实施基本保护的现有工具确实可以在一定程度上降低风险。但远不足以应对现在的 API 威胁。不能只靠这些工具提供保护。

企业应转为寻找一种全面的 API 安全解决方案，可以涵盖本买家指南中讨论的全部四个领域：发现、态势管理、威胁检测和修复以及安全测试。您不必丢弃在特定领域中行之有效的现有工具，只需要寻找可以与这些工具无缝集成的解决方案即可。

开始实施 API 安全措施并不意味着您需要分配大量资源。您可以先开展小规模、可衡量的试点，以解决安全堆栈中的漏洞。或者通过全面更新开启您的 API 安全旅程。每家企业各不相同。

随着针对 API 的攻击日益增加，您最重要的一步就是立即行动起来。希望本买家指南对您有所帮助。

阅读更多内容，详细了解 API 攻击方法、常见 API 漏洞以及如何保护您的企业。

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

Akamai 安全解决方案 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 9 月。