Akamai

白皮书

API 检测和响应的 11 个关键功能

发展您的 API 安全策略

前言

API 在各种应用程序中都发挥着至关重要的作用——不管是贵企业为客户构建的应用程序，内部使用的应用程序，还是提供给供应商使用的应用程序。API 的作用：在不同技术之间交换信息（通常是敏感数据）。API 所在的位置：不仅存在于您的应用程序中，还存在于您的云迁移、生成式 AI 工具和数字供应链中。

面临的挑战：API 还是企业攻击面中极具吸引力的攻击热点。

在企业争相创新的过程中，API 往往因开发仓促和测试不足，还带着配置错误和安全防护漏洞就被发布至生产环境。此外，这些 API 已形成了一种无序蔓延的态势，以至于安全团队对其大部分 API 资产都缺乏监测能力。如果缺乏合理的监测能力，企业便：

1. 无法检测不受管理、被遗忘以及持续暴露于敏感数据、互联网和攻击者风险之下的 API
2. 进而无法评估 API 风险，例如只有 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. 最终导致攻击面内到处都是以 API 为中心的漏洞，这些漏洞经常也很容易被攻击者利用

直到最近，许多企业还在安心地依赖一些常用工具来管理 API 和获取基本保护。然而，在过去 12 个月里，有 84% 的企业遭遇过 API 安全事件，较 2023 年 78% 的比例进一步上升，显然，企业要采取措施，改变这种局面。

随着 API 攻击的数量不断增加且手段日益复杂，企业应开始探索为 API 网关、Web 应用程序防火墙 (WAF) 以及 Web 应用程序和 API 保护 (WAAP) 平台等工具增加更多新的防护层。

这些新的防护层应该能够让您更好地监测环境中的所有 API 及其风险，包括大多数不受管理的 API，例如：

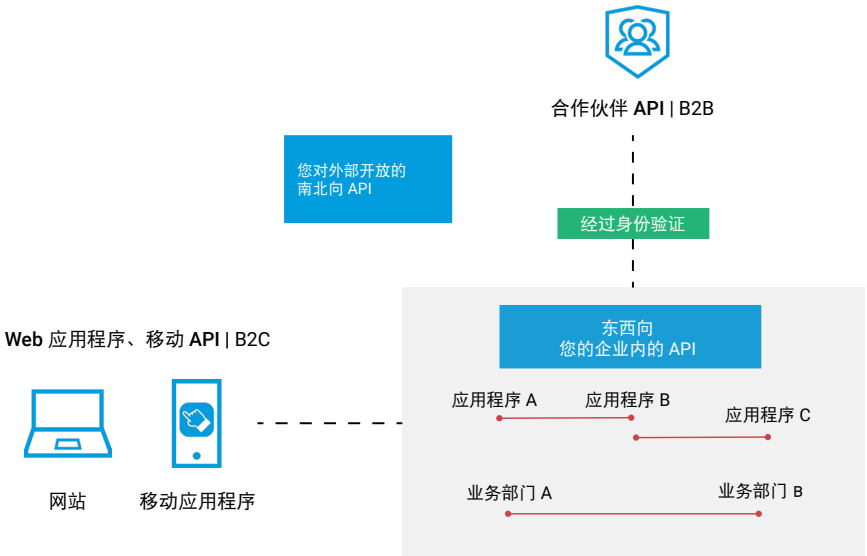
- 本已弃用但仍然处于活动状态的僵尸 API
- 没有文档记录并且应当清除或纳入正式管理流程的影子 API

各企业还需要更深入的功能来检测和应对 API 滥用及攻击，包括 OWASP 十大 API 安全风险中详细介绍的各种威胁。除了着眼于查找和修复 API 整个生命周期内的漏洞外，企业还应该从早期开发阶段到生产阶段，全程对 API 进行全面和严格的实时安全测试。

这是否意味着只要出现一个新问题，就要采用一种新工具？当然不是。与之相反，这更像是确保交响乐队的每一种乐器都有合适的人员演奏，他们不仅能够在正确的时间演奏正确的音符，还能够与其他成员精确配合。

在考虑如何为 API 保护堆栈增加新的防护层时，您需要考虑安全团队应对其他威胁时采用的深度防御方法，例如部署一系列控制措施来检测、防范和减轻勒索软件攻击的影响。这正是企业在考虑 API 时的所应采取的方式。

在本白皮书中，我们将探讨 11 项可以纳入 API 安全策略的关键功能，并以 API 威胁检测与响应为重点。



关键在于应用场景

API 威胁检测和响应在 API 安全策略中处于什么位置?

正如您可能已亲眼目睹的那样，凭借支持更多应用场景、加速变革、承载更多敏感数据以及向更多用户开放，API 已经改变了企业的运营方式。企业所创建的 API 通道数量远远超过了 Web 应用程序接口，这并不让人感到意外。随着这些激增的 API 与越来越多的核心业务数据和业务逻辑深度融合在一起，风险态势也相应变得更为复杂。

鉴于 API 广泛存在于已经受到安全团队保护的众多技术（即应用程序）之中，大多数类别的安全产品都会以某种方式支持 API 防护。然而，API 与应用程序不是一码事；在某些合规框架中，它们甚至被作为单独的资产列出。仅在现有应用程序的安全产品等防护系统中添加零散的 API 威胁防护功能的做法已变得捉襟见肘。虽然大多数企业通常也会关注 API，但 API 显然值得投入更多精力。现在的安全团队应该将 API 视为一种具有不同风险属性的单独资产类别，并获取能够大规模地发现和保护每个 API 的关键功能。

过去，如果某个企业有 API 清单并使用一些基本工具来进行 API 管理和保护，他们就能够防范已知的一系列常见 API 攻击。不幸的是，与公司一样，现在的攻击者往往也会进行创新，并同样会着眼于持续改进。

- 恶意攻击者在有条理地改进其手段，以绕过他们所知道的大多数企业保护 API 所依赖的工具。
- 与大多数企业使用 AI 的方式一样，攻击者也会通过生成式 AI 功能来获取全天候帮助，从而增强其有限的人员能力。
- 攻击者在越来越多地寻找企业 API 连接的数字供应链中的薄弱环节，比如某些没有将 API 保护视为优先事项的 B2B 合作伙伴。

例如，当客户和合作伙伴获得了 API 凭据但以未经授权的方式使用这些凭据时，就会产生某种形式的 API 滥用。还有一些方法可以劫持看似合法的 API 凭据或安全令牌。API 客户端实施中隐藏的漏洞是另一种攻击媒介，攻击者可能会利用此攻击媒介，以传统安全工具无法检测到的方式滥用 API。

好消息是，企业现在可以大规模采用一些必要的关键功能来保护 API，使其免受快速变化的攻击方法的影响。请继续阅读，详细了解您的团队可以如何着手使用 11 项关键功能，从而采取措施来保护 API 及其交换的数据免受攻击。

第 1 项关键功能
持续的 API 发现和态势管理

拥有整个企业内使用的 API 的完整清单并且持续更新这份清单，这是任何 API 安全策略的重要基础。道理很简单，因为企业只有在了解自己环境中的资产后才能保护这些资产。许多 API 安全产品声称可以在某种程度上实施 API 发现，但是仅限于按需发现或每日发现。企业平台的 API 发现功能很有必要包含以下几个方面：

- 全天候自动持续发现 API，包括仅使用一次的 API（按需发现或每日发现并不够）
- 发现不同技术环境和基础架构中的 API
- 发现新部署的 API 并与记录完备的 API 进行比较，以识别影子 API
- 对每个 API 服务和端点进行风险评分，这可以帮助安全团队和开发团队排除干扰，并优先处理那些一旦遭受入侵便会产生重大潜在影响的 API
- 检测已知 API 漏洞的实例，例如 OWASP 十大 API 安全风险中列出的漏洞

更好的监测能力
绝不会再忽视您的 API 清单

第 2 项关键功能
监测 API 行为

监测 API 的真实行为（API 调用）是 API 安全平台的一项基本功能。具备这种功能才能让安全、开发和运营方面的关键利益相关者查看和了解 API 的使用或滥用情况，以便他们在团队之间进行沟通并对案例展开调查。企业需要构建的具体可视化功能包括：

- **调查：**任何告警都应该包含针对每个调用检查原始 API 活动的功能，以识别告警的具体触发因素。
- **数据保真和数据丰富：**对于每次 API 调用，都应该要能知道用户是谁、他们使用了什么运算、访问或操作了哪些记录、使用了哪些标头和参数等。
- **数据隐私：**虽然数据保真很重要，但敏感数据不能静态存储。解决方案应该分析流量，并且仅发送相关元数据以更新仪表板。

第 3 项关键功能
通过与用户实体相关的背景信息发现 API 滥用尝试

安全团队需要能够顺藤摸瓜地追踪到执行恶意活动的实体（比如 IP 地址）以及业务流程实体（比如支付 ID ）。如果有其他的相关标识符提供 API 滥用的背景信息，同时还能将实例中来自不同 IP 的攻击关联起来，这种功能就会变得非常有价值。

假设某个未知用户在使用 /api/getpaymentID/50 作为其 ID 来调用一家零售公司的 API。在此情况下，该零售商的安全团队知道公司平台中的每个其他用户都与一类付款 ID 相关联。如果安全分析师突然看到该未知用户不断重复调用 API，并且每次都会稍微调整 ID 编号 (/api/getPaymentID/51 ⋯ 52 ⋯ 53 ⋯ 54)，这就是用户在试图滥用 API 的重要征兆。

一旦能够实时洞察非典型用户行为，就能阻止入侵尝试，使 API 攻击无法得逞。

$943,162

这是修复 API 安全事件的平均成本，此数据基于过去 12 个月表示曾遭遇此类事件的美国 CISO、CIO 和 CTO 的报告。

如需详细了解同行观点和经验，请访问《2024 年 API 安全影响研究》。

第 4 项关键功能
行为分析和检测

虽然分析来自用户实体的各个 API 调用甚至各个会话对安全团队有所帮助，但更重要的是拥有能够着眼于全局的全面 API 威胁检测功能。这些功能必须能够在整个 API 资产环境中深入了解行为模式和异常。要确定 API 的行为是否异常（表明它可能已遭到入侵），应该对较长时间段内的 API 使用情况进行分析，并通过长时间的全面行为跟踪来建立上下文基础。在安全团队持续监控行为以检测异常时，这可以为他们提供可靠的基准。

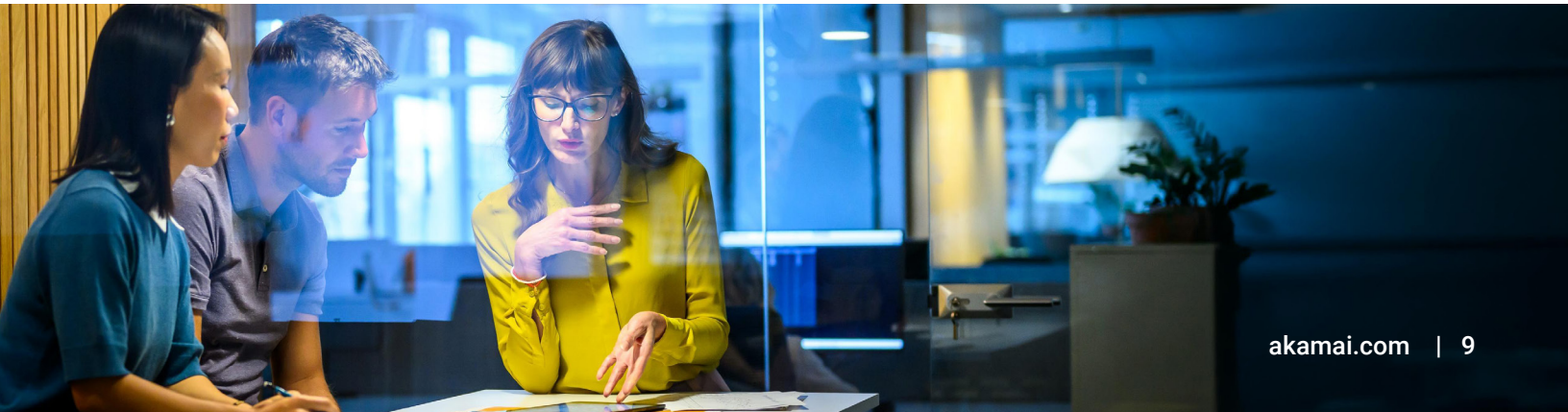
第 5 项关键功能
API 规范偏离检测

随着市场需求和业务要求的变化，API 也在不断变化。因此，企业需要持续发布新的端点实施来满足快速变化的企业需求、修复错误以及引入技术改进。根据 API 规范，紧跟这些变化对 API 文档进行同步更新至关重要，并且应该特别注意确保 API 流量始终符合其规范的要求。

要让 API 能够抵御滥用和攻击，企业应该寻找用于检测 API 规范偏离的功能。通过将实时 API 流量与已定义的规范进行持续对比，这可以帮助企业查明 API 文档中的任何差异或差距。

如果 API 规范偏离检测功能发现任何不匹配或未记录的端点在生产环境中遭到访问，它就会向开发人员和安全团队发出告警，让他们能够：

- 防患于未然
- 确保 API 按预期方式运行
- 增强这些 API 支持的应用程序的安全性
- 保持企业 API 生态系统的完整性



第 6 项关键功能
覆盖 B2B 和东西向 API

API 使用量增长最高的是 B2B 领域，包括面向内部和外部的应用场景。API 安全必须覆盖 B2B、机器对机器 API，包括南北向（面向外部）和东西向（面向内部）的实例。

虽然 B2C Web 应用程序受到 WAAP 和 WAF 平台保护，但一些非常敏感的 API 活动类型（例如，内部东西向 API 或通过 B2B API 向合作伙伴开放的专有应用程序功能）即使在经过 WAAP 时仍可能受到侵害。

通常，用户经过 B2B 合作伙伴 API 身份验证后，就会被认为是安全的，而不会进一步监控其相关活动。这造成了许多企业 API 安全态势中的严重漏洞。为了全面掌握 API 活动情况和更大范围的威胁态势，企业必须采用一种能够有效了解、观测和监控所有应用场景的方法。

第 7 项关键功能
有上下文、有意义的告警

一旦企业能够监测其 API 活动并实施大规模行为分析，API 活动的告警就变得更有意义。但是，您如何能够确保自己将注意力和资源集中在真正的 API 威胁上？攻击者置信度引擎可以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，以确定所检测到的运行时事件确实是由恶意活动引起的置信度。此功能有助于安全团队快速锁定关键威胁，并且应当辅以针对高概率攻击创建自动修复和通知流程的功能。

第 8 项关键功能
定制的自动响应

传统的内联 API 方法可以采取自动化操作来阻止可疑的 API 攻击，但前提是企业必须能够识别这类攻击。API 行为分析和异常检测是在更大的业务背景下长期实施的，这种检测深度有利于发现异常情况。这样企业就能够以更高的准确度实施各种自动化响应和定制响应。示例包括：

- 在支持的 API 网关和内容交付网络 (CDN) 边缘过滤器处阻止或限制流量
- 向安全和业务利益相关者发送电子邮件通知
- 为开发人员创建工单
- Webhook 的触发

随着 API 威胁的不断增长，企业能够采取什么措施来帮助捉襟见肘的安全团队最大限度地发挥其团队作用和能量？寻找自动化功能，通过简化多动作工作流的创建和管理来提高效率和生产力。正确的自动化功能应该提供无代码的可视化设计程序界面，该界面可以创建复杂的事件响应流程，并在您的核心 API 安全解决方案与各种第三方服务（包括 ServiceNow、Jira 和 Azure DevOps）之间同步事件相关数据。

第 9 项关键功能
API 流量分析

企业需要在不部署数据湖的情况下，能够对环境中的 API 流量进行不间断地记录、监测和分析。通过记录整个应用程序环境中符合特定标准的 API 数据流（包括典型和异常的 API 活动），企业可以更有效地搜寻威胁，同时管理可疑用户和异常 API 行为的相关风险漏洞。拥有能够根据特定应用场景进行量身定制的 API 流量审核功能非常重要，它让企业能够根据预先确定的过滤器和规则来捕获及保留流量。

第 10 项关键功能
严格的实时 API 测试

在争相创新的过程中，企业往往会将存在未检测到的漏洞和设计缺陷的 API 发布到生产环境中。而要避免产生这些问题，可以在开发过程中采用左移方法来进行 API 测试。核心功能包括：

- 运行模拟恶意流量（包括 OWASP 十大 API 安全风险中涵盖的类型）的自动化测试
- 依据已确立的治理策略和规则，对 API 规范进行检查
- 根据需求进行 API 测试，或者将 API 测试作为 CI/CD 管道的一部分

第 11 项关键功能
平台无关的保护

API 服务通常由企业内的不同团队使用多种平台和技术来实施。例如，有些 API 在本地实施，而其他 API 在公有云中运行。通常，企业会使用中间技术（例如，反向代理、API 网关、WAF 和 CDN），这些技术虽然提供了业务价值，但也增加了 API 监测的复杂度。

对于企业而言，这些技术能否支持 API 活动数据的访问至关重要。平台无关的 API 威胁防护方法可确保企业始终能够全面了解 API 活动，而不受实施细节或所用基础架构的限制。这将能确保以下这些方面的安全：

- 所有部门、收购的公司和各类环境
- 已批准的 API 和影子 API，无论它们是否使用 API 网关

此外，平台无关的方法也可以将监测能力扩展到南北向 API 之外，并包括公共、合作伙伴和内部东西向 API。

如果能够确保 API 威胁防护平台实现尽可能广泛的监测范围，不但可以帮助企业抵御外部攻击风险，还能够防止可能来自合作伙伴企业的内部威胁和 API 滥用。

结论

今天，在数字化和以云为中心的经济环境中，API 是企业服务客户、创造收入以及高效运营能力中的关键组成部分。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 成为重要的风险来源。

Akamai API Security 提供了本白皮书中介绍的所有 11 项关键功能，可帮助企业在其现有方法的基础上构建必要的功能，例如：

- 发现 API
- 评估风险（包括敏感数据相关风险）
- 检测 API 滥用和攻击
- 对 API 进行安全风险和漏洞测试

详细了解如何防范 OWASP 十大 API 安全风险。

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

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：25 年 01 月。

扫码关注 - 获取最新云计算、云安全与 CDN 前沿资讯