白皮书

API Detection and Response 的 10 大关键功能

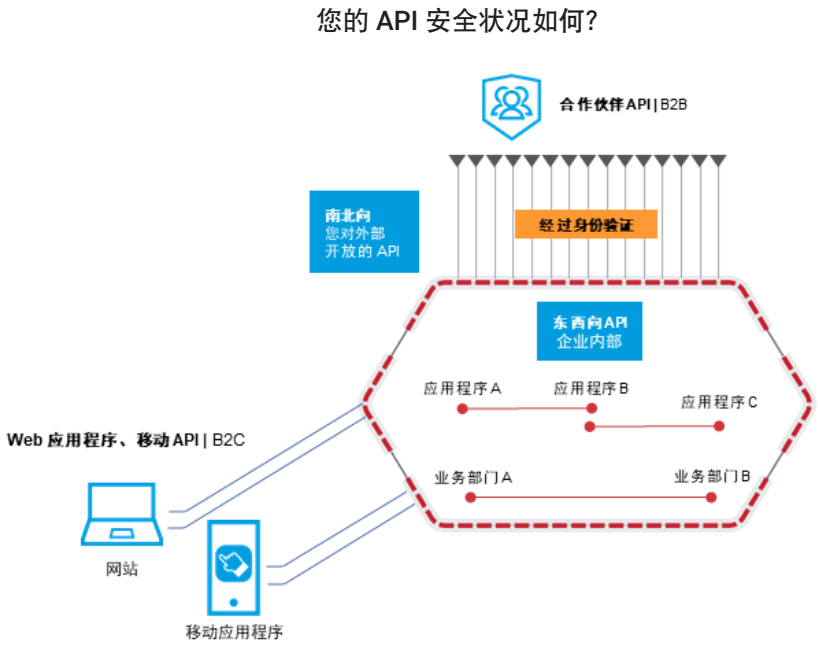
不断增强您的 API 安全策略

前言

API 是推动创新的关键环节，而企业对企业 (B2B) 和企业对消费者 (B2C) 应用程序是此次转型的核心所在。这意味着保护内部微服务之间和外部客户端及合作伙伴之间的关键通信（通常是敏感通信）非常重要。大多数企业现在都认识到，完善的应用程序安全策略对于长期业务成功而言必不可少。所以，为了降低应用程序安全风险，企业采用了 Web 应用程序和 API 保护 (WAAP) 平台、云安全功能和产品以及安全测试工具等各种安全技术。但企业还需要认识到，网络攻击也在演变，攻击者已经绕过 WAAP，将目标对准企业内部的 API。所以，我们有必要讨论一下如何调整 API 安全策略才能先发制人地应对这些威胁。

API 检测和响应在 API 安全策略中处于什么位置?

在过去几年里，企业所创建的 API 通道数量远远超过了 Web 应用程序接口，而且这些 API 包含越来越多的核心业务数据和业务逻辑。API 已经改变了企业的运营方式，因为它能支持更多应用场景、加速变革、承载更多敏感数据，并向更多用户开放。



随着 API 的使用日益广泛，大多数安全产品类别都会在一定程度上支持 API，但 API 属于不同的资产类别，甚至在某些合规框架中，API 被列为一种独立的资产。为传统安全产品（例如 WAAP 平台）增添 API 威胁防护功能并不能应对 API 资产带来的新挑战。安全部门必须将 API 视为单独的资产类别，并了解哪些关键功能可以全方位保护大量 API。

我们先从基本背景开始，谈谈 API 保护领域为应对新兴威胁而做出的改变。过去，如果企业拥有完整的 API 清单和强大的 WAAP 平台，通常就可以避开 API 威胁。但现在，攻击者已经能够绕过 WAAP，将目标对准企业及其合作伙伴的内部 API。

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。看似合法的 API 凭据或安全令牌也有可能被劫持。API 客户端实施中隐藏的漏洞是另一种可能被攻击者利用的攻击媒介，这会造成传统安全工具无法检测到的 API 滥用。

好消息是，企业现在可以大规模引入一些关键功能，特别是 API 检测和响应功能，来保护 API 免受新兴威胁的影响。在下面几页，我们围绕这些关键功能提出了谨慎的建议，意在帮助企业提高安全保护平台的效力，应对不断变化的 API 威胁态势。

关键功能 1
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 可能在本地实施，还有一些则可能在公有云中运行。企业还可能使用中间技术，例如反向代理、API 网关、Web 应用程序防火墙 (WAF) 和内容交付网络 (CDN)，这些技术增加了 API 监测的复杂度。

这些不同的技术能支持 API 活动数据的访问对于企业而言至关重要。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所有 API 活动，而不受实施细节或所使用的基础架构限制。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
- 经批准的 API 和影子 API，无论是否使用了 API 网关
- 监测能力扩展到南北向 API 以外，覆盖到公共 API、合作伙伴 API 和内部东西向 API

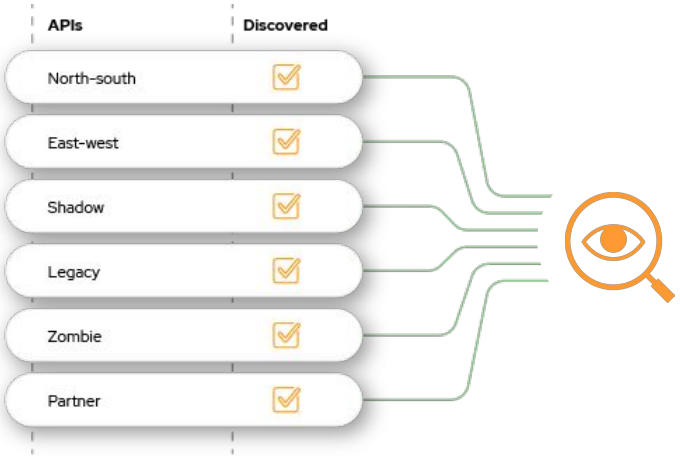
确保 API 威胁防护平台的监测范围尽可能广除了可以帮助企业抵御外部攻击风险，还能够防止可能来自合作伙伴企业的内部威胁和 API 滥用。

关键功能 2
持续的 API 发现和态势管理

拥有整个企业内所有 API 的完整清单并且持续更新这份清单是任何 API 安全策略的重要基础。道理很简单，因为企业如果不清楚自己的资产，就无法保护这些资产。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所有 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
- 检测已知 API 漏洞的实例，例如 OWASP □□ API □□□□中列出的漏洞

更好的监测能力
绝不会再忽视您的 API 清单

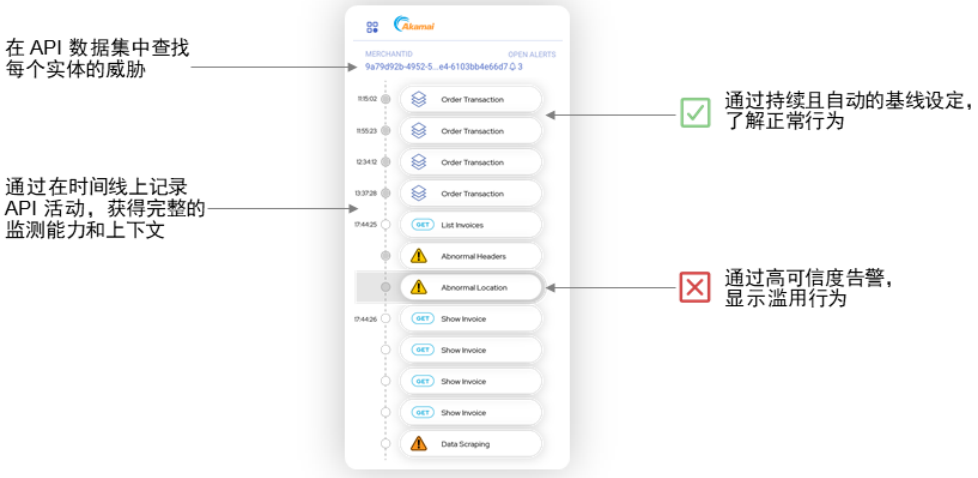


关键功能 3
API 行为可视化

显示实际 API 行为（API 调用）并使之可视化是 API 安全平台的基本功能。具备这种功能才能让安全、开发和运营部门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。
- **威胁搜寻：**历史数据应扩展到至少 30 天的滚动视图，能够查看所有 API 活动、查询时间范围和特定告警以外的调用。这个功能还有助于满足合规要求。
- **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：**尽管数据保真很重要，但敏感数据不能静态存储。需要对数据进行令牌化，来保持数据的丰富性而不存储敏感数据。
- **时间轴可视化：**应该为用户提供一个能按活动顺序轻松向前和向后移动的视图。

使用行为分析检测威胁



关键功能 4
跟踪多个用户实体

理解实体并且能够查看相关的 API 活动，就能获得任何使用或滥用行为的上下文信息，所以企业 API 保护平台必须足够成熟，能够单独跟踪每个实体。这样才能提供必要的上下文信息，因为一类用户的正常活动对另一类用户来说可能就是滥用的信号。能够查看时间轴上每个实体的活动，才能获得至关重要的监测能力和上下文信息。例如：

API 活动	参与者	实体	业务流程实体
示例	内部用户、B2B 合作伙伴、外部用户	IP 地址、API 令牌、商户 ID、会话 ID、租户 ID	付款 ID、发票 ID

关键功能 5
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。

尽管 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。

关键功能 6
行为分析和检测

分析单个 API 调用（或甚至单个会话）并不能检测复杂的 API 威胁。API 检测和响应需要深度理解行为的上下文信息并从中进行学习。为了解 API 行为是否异常（行为异常表明可能已受到攻击），有必要分析更长时间范围内的 API 使用情况。行为分析技术可确定正常用户行为的基准，并持续监控用户行为，以检测异常情况。

对典型的企业 API 活动执行这种级别的分析需要大量的存储和计算资源，而本地 API 安全工具规模有限，用来实施这样的分析并不现实。EDR 和 XDR 解决方案引领趋势，表明了执行有意义的行为分析需要采用软件即服务 (SaaS) 架构。云的性能和规模可以实现长期数据存储，同时能够支持这样的分析来确定一段时间内的正常用户行为，以便检测极其隐蔽的滥用信号。SaaS 方法还有其他优势，例如实施起来更快、更简单，而且具有更高的可扩展性和灵活性，能够应对 API 使用量的增长。

关键功能 7
有上下文、有意义的告警

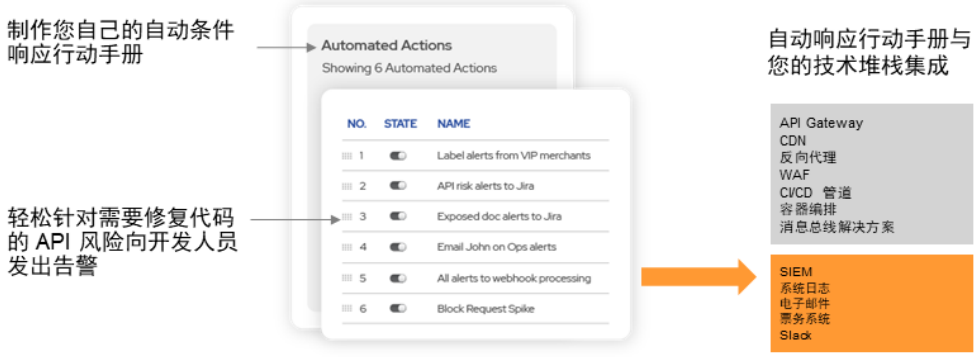
一旦企业能够监测所有 API 活动并实施大规模行为分析，API 活动的告警就变得更有意义。企业可以采用更抽象的安全监控方法，从而不再需要预测每种可能的攻击方法。通过建立正常行为的基准并检测异常行为，还可以检测任何模式或签名通常无法检测到的 API 滥用。此外，企业还能够回溯攻击并了解告警之前的情况，从中获得关于 API 资产的使用和滥用的重要信息。

关键功能 8
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 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
- 开发人员的工单创建
- Webhook 的触发

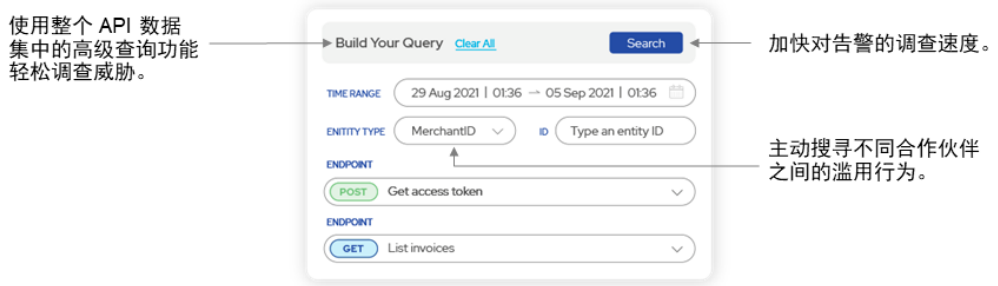
可根据业务流程定制响应



关键功能 9
主动调查和威胁搜寻

等到安全事件发生后再采取行动，这样的代价是很多企业都无法承担的。更有效的方法是识别不利活动并主动搜寻这类活动。例如，在告警提示检测到一个 API 的滥用时，通过采用主动威胁搜寻对另一个 API 执行同样的检测，也可能发现滥用行为。因此，API 威胁防护平台除了针对活动事件生成告警之外，还应该包含搜寻特定类型行为的功能。威胁搜寻功能需要访问历史数据才能发现隐藏在 API 活动数据中的滥用行为。单一请求解决方案无法让数据变得更加丰富以提供上下文信息，因而无法呈现事件的完整脉络。威胁搜寻和调查建立在历史数据的基础上。

轻松执行调查和威胁搜寻



关键功能 10
可观测的数据湖

在强大的 API 安全策略的所有功能中，上下文是长期保护任何 API 的关键。要想维持足够的上下文来观察威胁、识别潜在漏洞并在发生攻击时进行故障排除，最好的办法是记录所有 API 行为并保留此活动的待办事项列表。如果拥有与 API 安全解决方案相关的数据湖，便可实现这一点。数据湖应该尽可能提供更多历史细节，来为策略提供可靠的数据。虽然将基本请求数据输入机器学习模型可能会有帮助，但拥有请求参数等详细信息，企业就能根据历史数据采取切实的行动，以抵御未来的威胁和攻击。

1 平台无关的保护	确保 API 威胁防护平台的监测范围尽可能广可以帮助企业抵御威胁和避免滥用。
2 持续的 API 发现和态势管理	拥有整个企业内所有 API 的完整清单并且持续更新这份清单非常重要，因为企业如果不清楚自己的资产，就无法保护这些资产。
3 API 行为可视化	拥有监测能力才能让安全、开发和运营团队的关键利益相关者查看和了解 API 的使用或滥用情况，从而在团队之间进行沟通并对案例展开调查。
4 跟踪多个用户实体	理解实体并且能够查看相关的 API 活动，就能获得任何使用或滥用的上下文信息，所以企业 API 保护平台必须足够成熟，能单独跟踪每个实体。
5 覆盖 B2B 和东西向 API	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。
6 行为分析和检测	为了解 API 行为是否异常（行为异常表明可能已受到攻击），有必要分析更长时间范围内的 API 使用情况。行为分析技术可确定正常用户行为的基准，并持续监控用户行为，以检测异常情况。
7 有上下文、有意义的告警	一旦企业能够监测所有 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。企业可以采用更抽象的安全监控方法，从而不再需要预测每种可能的攻击方法。

8 定制的自动响应	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。
9 主动调查和威胁搜寻	等到安全事件发生后再采取行动，这样的代价是很多企业都无法承担的。更有效的方法是识别不利活动并主动搜寻这类活动。
10 可观测的数据湖	要想维持足够的上下文来观察威胁、识别潜在漏洞并在发生攻击时进行故障排除，最好的办法是记录所有 API 行为并保留此活动的待办事项列表。如果拥有与 API 安全平台相关的数据湖，便可实现这一点。

如果您认为这些建议有用，不妨继续了解 Akamai 的 API Security 解决方案，确保为您的企业应用强大的 API 安全策略。

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。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：2023 年 12 月。

扫码关注 · 获取最新CDN前沿资讯