Akamai

白皮书

API 安全基本现状：增长知识，保护企业

前言

API 已从一种实施细节迅速演变成具备战略价值的数字化创新推动力。每当有客户、合作伙伴或供应商与企业进行数字互动时，后台都会有相应的 API 来帮助实现数据的无缝交换。

随着 API 数量激增，风险也随之增大。当今企业争相快速创建和发布新的应用程序和 AI 增强型服务，然而匆忙之下，API 往往出现配置错误、缺乏安全控制措施，导致攻击者可以轻而易举地对其发动攻击。

因此，API 已经成为主要攻击媒介，许多安全团队不得不努力恶补，以完善 API 安全策略。因此，API 安全防护迅速成为 IT 和安全主管的首要任务。

无论您是想了解 API 安全基础知识，还是想整理一份合适的提问清单，本指南都能为您提供必要的详细信息，包括：

- API 的不同类型
- API 安全对当今企业意味着什么
- 应对 API 安全风险的最佳实践
- 常见的 API 攻击和滥用方法

您可以直接查看第 10 页上的 API 安全最佳实践。

目录

API 基础知识

什么是 Web API?

Web API 应用程序编程接口 (API) 由已定义的请求响应消息系统的一个或多个端点组成，通常以 JSON 或 XML 表示，并通过网络（最常见的是基于 HTTP 的 Web 服务器）对外开放。

换句话说，大多数人听到“API”时想到的就是 Web API。它是端点的集合。端点由资源路径、可对这些资源执行的操作，以及资源数据的定义（JSON、XML、Protobuf 或其他格式）组成。

Web API 不同于其他 API（例如操作系统或在同一台机器上运行的应用程序库所公开的 API），但“API”这个通用术语通常是指基于 HTTP 的 (Web) API，尤其是在企业数字化转型和 API 安全领域。

最常见的 API 类型有哪些?

下面的术语表解释了 API 实施中用到的各种 API 使用模式和技术方法。Web API 的定义是基于 HTTP 的 API，目前常见的四种主要类型是 RESTful、SOAP、GraphQL 和 gRPC。表中给出了这些常见类型及其他类型 API 的定义。

API 使用模式	描述
公共 API	通过互联网向所有开发人员免费提供和共享的 API
外部 API	此类 API 是通过互联网开放的 API，这个术语通常可与“公共 API”互换使用
私有 API	在受保护的数据中心或云环境中实施的 API，供受信任的开发人员使用
内部 API	这个术语通常可与“私有 API”互换使用
第三方 API	提供对第三方专门功能和/或数据的编程访问，以在应用程序中使用
合作伙伴 API	一种第三方 API，有选择地提供给已授权的业务合作伙伴使用
经过身份验证的 API	只有已获准访问的开发人员才能访问的 API（攻击者可能窃取凭据而对这类 API 进行未经授权的访问）
未经身份验证的 API	无需特定凭据也可通过编程方式访问的 API
HTTP API	这类 API 使用超文本传输协议作为 API 调用的通信协议

RESTful API	RESTful API 易于供现代前端框架（例如 React 和 React Native）使用，并可促进 Web 应用程序和移动应用程序的开发；它们已成为各类 Web API（包括用于 B2B 的 Web API）的事实标准
GraphQL	GraphQL API 是 Facebook 开发的较新标准，通过单个 POST 端点（通常为 /graphql）提供数据库访问能力；它解决了 RESTful API 的一个常见问题，即填充一个用户界面页面时需要执行多次调用
SOAP	SOAP 使用详细的可扩展标记语言 (XML) 进行远程过程调用 (RPC)。在旧版 API 中仍然可以找到它
XML-RPC	XML-RPC 是通过互联网进行过程调用的一种方法，使用 XML 进行编码并用 HTTP 作为通信协议
gRPC	gRPC API 是 Google 开发的 HTTP/2.0 高性能二进制协议，主要用于东西向（内部网络内部的）通信
OpenAPI	OpenAPI 是 API 的一种描述和文档规范。还有两个术语比较重要——Swagger 指的是原始规范，而 OpenAPI 指的是 OpenAPI 计划制定的开放标准

API 和端点有什么区别?

人们在使用“API”这个术语时，通常他们真正想说的是单个 API 端点。API 有时称为服务或 API 产品，是为业务功能服务的端点集合。另一方面，单独一个端点是指一项资源（或资源路径，也称为 URI 或统一资源标识符）和对资源执行的操作（创建、读取、更新或删除）。在 RESTful API 中，这些操作通常对应于 HTTP 方法（POST、GET、PUT 和 DELETE）。

什么是南北向 API?

这些 API 是企业供外界访问的 API，主要用于与业务合作伙伴开展业务。这种情况称为 API 开放。例如：

> **支持开放银行业务的银行可能通过 API 向其他金融科技企业或金融服务企业开放其帐户。**

> **医疗保健企业可能通过 API 向保险公司和其他医疗企业开放患者记录。**

> **酒店企业可能通过 API 向旅行社或旅游信息采集平台开放其预订系统。**

API 是支持不同企业交换数据的连接纽带。南北向 API 通常被认为是安全的，因为 API 访问已获得授权并已经过身份验证。这些 API 通常增长极快且数量庞大，因此对大多数企业而言，构成了最大的攻击面。

什么是东西向 API?

这些 API 是企业内部使用的 API，不应允许企业外部的任何人访问。它们将内部应用程序或者业务单位（部门）连接起来。开发人员可能意外地出现配置错误，允许东西向 API 被访问。这些 API 不应该被外部实体访问，甚至不应该被外部实体知晓，而一旦攻击者发现可通过互联网访问的东西向 API 时，就会发生入侵。

B2C API 和 B2B API 有什么区别?

企业对消费者 (B2C) API 为 Web 应用程序和移动应用程序提供支持。这些 API 通常由现代前端客户端使用，是为了让经过身份验证的最终用户能够访问公司的业务功能。

企业对企业 (B2B) API 是企业与企业之间为了开展业务而提供的，有时也用于为共同的客户提供价值。

B2B API 有助于简化企业与其供应商、经销商和其他合作伙伴的合作方式，并让企业能更轻松地为客户提供更好的体验。

B2B API 的例子包括：

开放银行 API

供应链管理 API

贸易伙伴之间的电子开票和付款

API 的使用者千差万别，因此用于保护这些 API 的安全控制措施也各不相同。直到不久前，网络安全行业的关注点仍然仅限于 B2C 应用场景。但即便是在这些应用场景中，重点也不是保护 B2C API，而是保护 Web 应用程序。通常用于保护 B2C Web 应用程序的安全工具和控制措施具有一定的优势（如 Web 应用程序防火墙 [WAF]/Web 应用程序和 API 保护 [WAAP]），但无法提供保护 B2C API 免受攻击所需的监测能力、实时监控与保护。

保护 B2B API 的难度与日俱增。这些 API 往往缺乏基本的保护机制，更容易成为攻击者的目标。早期的 API 安全工具对 B2B API 的监测能力有限，难以保障代表共享用户执行批量数据访问的 API 的安全性（例如在开放银行业务中，金融科技公司和金融机构双方同意共享客户数据）。不过，较新的 API 安全解决方案提供了行为分析功能，可以辨别异常活动，从而有效解决这些问题。

私有 API 和公共 API 有什么区别?

私有 API 有时也称为内部 API，供公司的开发人员和承包商使用。私有 API 通常是面向服务的架构 (SOA) 计划的一部分，用于支持不同的部门或业务单位相互高效访问彼此的数据，从而简化内部开发流程。

相比之下，公共 API 也称为外部 API，面向公司外部的使用者开放。这些 API 作为开放 API，在极端情况下，可供任何人自由使用。但无论如何，这些 API 都需要更严格的管理和完备的文档，才能给公司外部的工程师使用。

必须指出的是，可通过互联网访问的私有 API 从严格意义上讲不是真正的私有 API。以 ACME 的 B2C API 为例，这些 API 由 ACME 的工程师在内部开发，仅供 ACME 移动应用程序使用。您可能会认为这是私有 API，但其实该 API 的流量来自互联网（“公司外部”），因此它并不是真正的私有 API，只是未向外部受众发布而已。黑客会频繁攻击此类 API，他们通过拦截流量并对移动应用程序进行逆向工程，来找到对应的 API。

API 安全解析

什么是 API 安全?

API 安全是一种策略，用于监测、严格测试和保护整个企业范围内的每一种 API。这其中包括与应用程序、业务流程和云工作负载密不可分的 API。然而，考虑到内部和外部 API 的产生速度极快、数量极其庞大，很难完全了解企业的整个 API 环境。许多企业缺乏相关的监测能力，并不了解其实际拥有多少 API，也不知道哪些 API 在被调用时会返回敏感数据。要想确定并降低 API 安全风险，需要采取足够成熟的安全控制措施，从而提供这种监测能力和数据分析能力。需要保护的 API 可包括：

- 让客户或业务合作伙伴能够轻松访问数据的 API
- 通过业务合作伙伴使用的 API
- 在内部实施和使用的 API，让应用程序功能和数据能够以标准化和可扩展的方式供各种系统和用户界面使用

有效的 API 安全策略必须包含系统化的方法，以便评估风险和潜在影响并执行恰当的抵御措施。评估风险的第一步是为企业发布和使用的所有经批准和未经批准的 API 建立完整的清单。此清单应包含以下属性：

- 数据分类，至少区分“不敏感”、“敏感”和“非常敏感”的数据
- 风险指标，例如 API 漏洞和配置错误

此外，API 监测和风险抵御措施必须考虑各种潜在的威胁，包括：

- 检测并防止使用未经批准的“影子 API”（请参见侧栏）
- 识别并修复可能被攻击者利用的 API 漏洞和配置错误
- 防止 API 滥用实例，例如业务逻辑滥用和数据抓取

API 安全与应用程序安全有何不同？

虽然 API 安全和传统应用程序安全是两个相互关联的领域，但 API 安全是一个独特的挑战，主要有两个原因，即规模和复杂性。

更大的防护规模

API 使用量快速增长有三个因素：

1. 微服务（一种强制使用 API 进行服务间通信的架构）的使用日益广泛。
2. 在直接用户渠道中，有 React、Angular 和 Vue 等现代前端应用程序框架使用 API 并且正在取代传统 Web 应用程序。
3. 为了适应全新的渠道（例如合作伙伴、物联网和业务自动化），也会添加 API。

灵活性导致复杂性

与 Web 应用程序不同，API 可以在许多不同的场景中以编程方式使用，这使得区分合法使用与攻击和滥用十分困难。

有没有安全团队应该理解的 API 分类法？

以下是安全语境中可能出现的 API 常见分类和说明。

经批准的 API

已发布的 API（带有 Swagger 文档或类似文档）

未经批准的 API

- 影子 API
- 恶意 API
- 僵尸 API
- 隐藏 API

过时的 API

- 已弃用的 API
- 旧版 API
- 僵尸 API
- 孤立 API

保护 API 的最佳实践有哪些?

要想加强 API 安全性，应从以下最佳实践入手：

- 将 API 安全标准和实践与企业的软件开发生命周期进行整合。
- 将 API 文档和自动化安全测试纳入持续集成/持续交付 (CI/CD) 管道。
- 确保对 API 应用适当且有效的身份验证和授权控制。
- 实施速率限制措施，帮助防止 API 滥用或崩溃。
- 使用专用网关和/或内容交付网络增强速率限制和其他应用程序级措施，以降低分布式拒绝服务 (DDoS) 攻击的风险。
- 让 API 安全测试成为更大范围的应用程序测试流程中不可或缺的一部分。
- 执行持续的 API 发现。
- 实施系统化的方法来识别和修复常见 API 漏洞，包括 OWASP 十大 API 安全风险清单。
- 使用基于签名的威胁检测和预防，作为针对已知 API 攻击的基准级防护。
- 利用 AI 和行为分析来增强基于签名的检测，使 API 威胁检测的扩展性、准确性和业务相关性更强，并且能够抵御新型威胁。
- 确保 API 安全监控和分析流程持续数周并覆盖多个 API 会话。
- 作为对 API 安全监控和告警的补充，为威胁搜寻人员、开发人员、DevOps 和支持人员提供对 API 清单和活动数据的按需访问权限。

实施这些 API 安全最佳实践的能力取决于您在朝着成熟的 API 安全策略发展的过程中所处的阶段（请参见侧栏）。

API 安全成熟度的各个阶段

第 1 阶段：监测和发现

您在使用自动化方法发现所有 API 及其支持的微服务。覆盖广度至关重要，因为被忽视的 API（例如不再使用的 API）是攻击者的主要目标。

第 2 阶段：测试

您需要测试所有 API，以确保其代码编写正确，并且能够执行预期功能。在这一成熟度阶段中，在部署 API 之前能够执行测试就是最高的成熟水平；这样可以在 API 用于生产环境之前消除风险，而且在这个阶段中，无论需要执行何种修复，成本都要更低。

第 3 阶段：风险审计

您需要持续审计整个 API 环境，以发现配置错误的 API 或其他错误。审计还能确保对每个 API 进行充分记录，并确定它们是否包含敏感数据，或者是否缺乏适当的安全控制措施。

第 4 阶段：运行时保护

您使用的解决方案具有自动运行时保护功能，可以区分正常和异常的 API 活动。通过这种方式监控 API 交互，您就能实时检测到指示威胁的行为。

第 5 阶段：响应

您有应对可疑 API 行为的解决方案，例如 WAF 或 API 网关，可在可疑流量访问关键资源之前将其拦截。您的解决方案使用自定义的自动化规则。

第 6 阶段：搜寻威胁

您定期对既往威胁数据进行取证分析，以了解告警是否正确识别了威胁，以及是否出现了能够结合利用复杂工具和人工智能主动搜寻威胁的模式。

API 安全风险和滥用

什么是 API 漏洞?

API 漏洞是一种软件错误或系统配置错误，可能导致攻击者利用这类错误来访问敏感应用程序功能或数据，或者造成 API 滥用。OWASP 十大 API 安全风险清单十分实用，其中概括了一些被广泛滥用的 API 漏洞，这些也是企业应该尽力识别和修复的漏洞。

OWASP 十大 API 安全风险清单是否记录了所有 API 漏洞?

对于希望改善 API 安全状况的企业来说，OWASP 十大 API 安全风险清单是个很好的起点。清单中的类别涵盖了各种可能的 API 风险。但是，OWASP 十大 API 安全风险清单所包含的类别十分广泛，因此有必要深入研究每个类别的子领域。API 攻击者经常会利用 OWASP 中广泛涵盖的授权问题，但也有一些 API 风险完全不在 OWASP 十大 API 安全风险类别中，例如逻辑错误的滥用。

API 滥用方式有哪些?

API 会受到多种方式的攻击和滥用，以下是其中一些常见的例子：

- **漏洞利用：**底层基础架构中的技术漏洞可能会导致服务器受损。示例包括 Apache Struts 漏洞（CVE-2017-9791、CVE-2018-11776）和 Log4j 漏洞（CVE-2021-44228）。

- **业务逻辑滥用：**逻辑滥用是指攻击者利用应用程序设计或实施的缺陷来引发意外行为和未经批准的行为。这些场景会给 CISO 及其团队带来压力，因为传统的安全控制措施对其毫无用处。

- **未经授权的数据访问：**API 滥用的另一种常见形式是利用被破坏的授权机制来访问原本不应该访问的数据。这些漏洞有很多名称，例如失效的对象级授权 (BOLA)、不安全的直接对象引用 (IDOR)，以及失效的功能级授权 (BFLA)。

- **帐户接管：**在凭据被盗乃至 XSS 攻击之后，帐户可能会被接管。一旦发生这种情况，即使是编写得最好、安全性最高的 API 也可能被滥用。利用提供行为分析功能的 API 安全解决方案，可以将经过验证的活动与非法使用区分开来。

- **数据抓取**：如果企业通过公共 API 提供数据集，攻击者就可能积极查询这些资源，以便批量捕获大体量、有价值的数据集。

- **业务拒绝服务 (DoS)**：API 攻击者如果请求后端执行繁重任务，可能引发应用层的“服务侵蚀”或完全拒绝服务（GraphQL 中十分常见的一个漏洞，但任何资源密集型 API 端点实施都可能发生这种情况）。

什么是僵尸 API?

在不断变化的市场和业务需求推动下，API 也在不断演变。为了满足新的业务需求、修复错误和实现技术改进，企业不断发布新的端点实施，这些端点的旧版本会被弃用。但管理旧端点的停用过程并非易事。那些本应弃用的端点经常会继续存在而且可以访问，这些端点被称为僵尸端点。

如何找到各种类型的影子 API?

在企业范围内寻找影子 API 的方法之一是提取和分析您的网络上的 API 流量。API 流量来源的示例包括：

收集到所有可用源的原始数据后，可以使用 AI 技术将其转换为全面的清单，其中包含所有 API、端点和参数。在此基础上，可以执行进一步的分析来对这些元素进行分类，并识别应予消除或纳入正式治理流程的影子 API。

如何保护内部 API 和 B2B API?

这其实取决于“内部”的定义。有些团队将通过互联网向自己企业的 Web 应用程序和移动应用程序开放的 API 称为“内部 API”。虽然这些 API 的文档确实可能只有公司员工和承包商才能访问，但黑客已经擅长于分析应用程序并通过应用程序反汇编工具包和代理（例如 Burp Suite）对 API 进行逆向工程。

然而，如果“内部 API”的定义为无法从企业外部访问的东西向 API，则主要威胁就只剩下内部威胁。您应该像保护大多数其他 API 一样，保护东西向 API 和 B2B API：首先要确保软件开发生命周期 (SDLC) 的安全，然后确保访问经过身份验证和授权。您还可以实施管理配额、速率限制和尖峰抑制。此外，您还可以利用 WAF/WAAP，保护您的 API 避免已知威胁的侵扰。对于 B2B API，应考虑添加严格的身份验证机制，例如 mTLS，因为相关事务较为敏感，而且往往属于批量事务。

对于东西向和 B2B API，我们都建议采用行为分析方法，特别是在涉及许多实体时更应该如此，因为这可能会导致难以区分合法行为与非法行为。例如：

> **您如何确定特定合作伙伴的 API 凭据是否已遭到泄露?**

> **您如何判断开票 API 是否被合作伙伴滥用，特别是通过枚举发票编号来窃取帐户数据?**

保护 B2B API 和东西向 API 需要业务上下文，而业务上下文无法通过单独分析 IP 地址和 API 令牌等技术元素来获得。利用机器学习和行为分析来了解业务相关实体，这是有效了解并管理风险的唯一方法。有了用户或合作伙伴等特定实体甚至业务流程实体（发票、付款、订单等）正常使用 API 的业务上下文和历史基准，就有可能发现原本无法检测到的异常情况。

API 网关能否提供足够的风险防护能力?

许多企业都将 API 网关作为 API 安全防护的战略性措施。大多数 API 网关都具有丰富的集成安全功能，其中第一个是身份验证（如果可以利用 OpenID Connect，还有授权功能），企业应对这些功能加以利用。然而，仅仅在 API 网关执行身份验证、授权和配额管理并不够，原因如下：

API 网关的发现缺口：API 网关只能监测和控制在网关配置中可以管理的 API，无法有效检测影子 API 和端点。

API 网关的安全缺口：API 网关可以执行身份验证，并在某种程度上执行授权方案，但不会检查有效负载（就像 WAF 和 WAAP 所做的那样），也不会通过分析行为来检测滥用。

最常见的 API 配置错误有哪些?

鉴于 API 的使用方式多种多样，可能的 API 配置错误几乎数不胜数。但配置错误也存在一些共同之处：

身份验证失效或无身份验证

身份验证是保护通过 API 公开的敏感数据的基础。第一步是确保所有承载敏感数据的 API 一开始就设置了身份验证。但保护身份验证机制也很重要，可通过速率限制降低暴力破解攻击和撞库攻击的风险，并防止攻击者使用窃取的身份验证令牌。有时，配置错误可能会导致 API 使用者绕过身份验证机制，这类错误通常与令牌管理相关（例如有些众所周知的 JWT 验证问题，或不检查令牌范围）。

授权失效

API 最常见的一个用途是允许使用者访问数据或内容，包括敏感信息。而授权是在公开数据之前验证 API 使用者是否有权限访问这些数据的过程。授权可以在对象级或资源级进行（例如，我可以访问我的订单，但不能访问其他人的订单），也可以在功能级进行（管理功能就是常见的例子）。由于存在大量的边缘情况和条件，而且微服务之间的 API 调用流程多种多样，因此很难确保授权不出错。如果没有集中式授权引擎，API 实施可能会包含其中一些漏洞，例如 BOLA 和 BFLA。

安全配置错误

除了前面提及的身份验证和授权问题外，还可能存在多种类型的安全错误配置，包括不安全的通信（例如，未使用 SSL/TLS 或使用了易受攻击的密码套件）、不受保护的云存储，以及过度宽松的跨域资源共享策略。

缺乏资源和速率限制

如果 API 的实施对 API 使用者可以进行的调用次数没有任何限制，攻击者可能会将系统资源耗尽，导致服务降级或完全 DoS。至少必须对任何未经身份验证的端点的访问实施速率限制（其中身份验证端点至关重要），否则必然会发生暴力破解攻击、撞库攻击和凭据验证攻击。

什么是 API 攻击?

API 攻击指的是企图将 API 用于恶意或其他未经批准的目的。API 攻击有多种形式，包括：

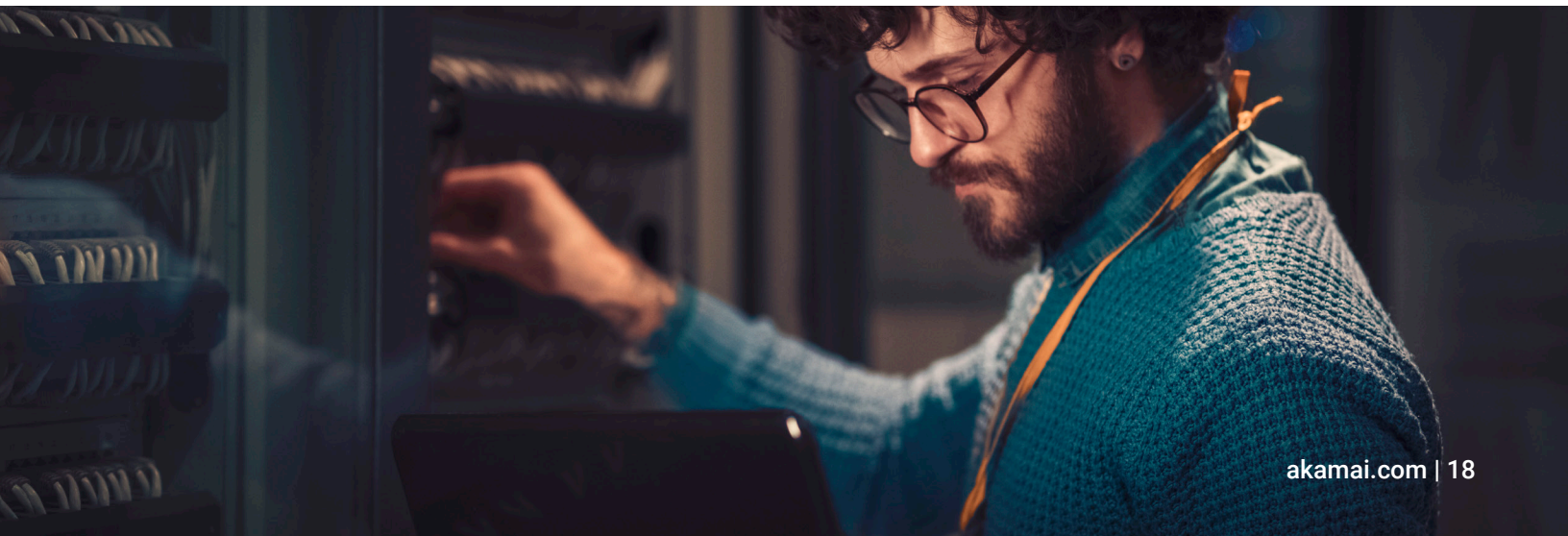
- 利用 API 实施中的技术漏洞
- 使用窃取的凭据和其他帐户接管技术伪装成合法用户
- 滥用业务逻辑，从而以无法预料的方式使用 API

什么是 API 的撞库?

网站和软件即服务 (SaaS) 平台泄露用户 ID 和密码信息已成为一种常态。通常，这些事件会导致大量凭据在网上大范围共享。撞库是黑客使用以前入侵的网站泄露的身份验证凭据，对其他网站执行自动登录的做法。这种方法的前提是有一定比例的用户在多个网站上使用相同的凭据。攻击者越来越多地直接攻击 API，将 API 身份验证机制作为攻击目标。这样做可以更轻松地执行自动攻击，因为创建 API 的目的就是为了方便使用。

什么是经由 API 的数据外泄?

数据外泄是 API 攻击和滥用得手后的常见后果。在某些情况下，这是指攻击者通过 API 攻击窃取高度敏感的非公开信息。不过，也可能指的是不太严重的 API 滥用类型，包括对公开可用数据进行侵略性数据搜索，以汇总有价值的大型数据集。



API 安全解决方案和趋势

API 安全领域有哪些最新趋势?

以下是安全主管在制定 API 安全策略时应考虑的主要趋势：

行为分析和异常检测：企业不再试图预测可能的攻击，也不再只依靠基于签名的检测和预定义策略（例如 WAF）来降低风险，而是越来越多地添加机器学习和行为分析功能，以在业务上下文中查看 API 活动并检测异常。

从本地过渡到 SaaS：许多第一代 API 安全产品都是部署在本地，但基于 SaaS 的方法因速度快、易于部署并且能够大规模利用机器学习而越来越受欢迎。

分析的时间范围更大：企业逐渐摒弃分析单个 API 调用或短期会话活动的 API 安全防护方法，转而采用能分析几天甚至几周 API 活动的平台，利用这些平台完成基本的自动化 WAF 策略优化以及执行行为分析和检测异常等多方面的操作。

DevSecOps——考虑非安全利益相关者：为降低 API 风险，企业可以加强 API 安全防护策略和工具与参与创建、实施和配置 API 的开发人员和系统之间的联系，这是一种非常好的方法。

API 赋能的 API 安全策略：虽然检测和抵御活跃 API 攻击和滥用实例至关重要，但有远见的企业正在想方设法对 API 安全数据和见解使用按需访问策略，以改进威胁搜寻、事件响应和 API 开发实践。

什么是基于签名的 API 安全防护?

基于签名的 API 安全防护技术会监控已知的攻击特征和模式，并在观察到匹配项时生成安全告警并做出其他自动响应。这是 WAF 的典型特征。就基于签名的检测而言，价值：如果企业知道传入 API 流量遭到入侵或行为异常，可以使用基于签名的 API 安全技术立即加以阻止。

您需要找到一种 WAF，它应该是更广泛的 WAAP 解决方案的一部分，能够通过机器学习提供高级检测能力，从攻击签名模式中学习，并可保持规模化敏捷性。如果 WAAP 与 API 安全解决方案集成，而且该解决方案具备行为分析和定制响应功能，就能两全其美。这些解决方案相结合，可以实现内部和外部的完整的 API 监测、检测和响应能力。

什么是 API 检测和响应?

API 检测和响应是 API 安全防护的新兴类别，它更注重对历史数据进行深入分析，以便：

- 确定所有 API 使用者的行为基准
- 检测预示潜在 API 滥用和误用的攻击和异常

只有在 SaaS 模式下才能实现有效的大规模 API 检测和响应，因为需要大型数据集来支持资源密集型机器学习技术。

什么是高级 API 威胁防护?

高级 API 威胁防护是基于 SaaS 的 API 安全方法，这种方法将行为分析与威胁搜寻结合在一起，以便：

- 发现企业使用的所有 API，包括影子 API 或僵尸 API
- 将机器学习运用到业务上下文，从中了解 API 的使用和滥用情况
- 对 API 和 API 活动数据执行行为分析和威胁搜寻

什么是 API 安全防护平台?

API 安全平台是一种基于 SaaS 的产品，经过特别设计，能够：

- 为整个企业内使用的所有 API（无论是否经过批准）创建持续更新的清单
- 分析 API 及其使用情况，以发现业务上下文并确定预期行为的基准
- 检测 API 使用中的异常情况，并在必要时向安全信息和事件管理 (SIEM) 以及安全编排、自动化和响应 (SOAR) 工作流提供告警和支持数据
- 允许安全利益相关者和非安全利益相关者按需访问 API 清单、活动和威胁信息

什么是 API 安全防护公司?

现在，IT 和安全领导者正以更具战略性的方法使用 API，他们可能需要专业 API 合作伙伴的支持。最常见的三种 API 公司类型是：

- API 网关公司，提供集中接受 API 调用并将调用发送到适当的后端资源和微服务的技术
- API 安全平台公司，确保组织了解所有活跃 API 及其潜在风险，能够检测攻击和滥用实例、实现全面的安全测试，并提供有关 API 使用情况的丰富数据
- WAAP 和 API 安全平台公司，可以帮助无缝传输 API 流量数据，同时仍提供发现平台内外 API 的能力；这是供应商整合和弥合数字鸿沟的理想选择

什么是 API 中的威胁搜寻?

威胁搜寻则会主动搜索未知威胁或先前未检测到的威胁。如果希望识别可能未曾见过的新兴威胁并提前实施抵御措施，避免其造成重大损害，这种主动式方法至关重要。威胁搜寻中使用的关键技术之一是行为分析。这涉及分析 API 的行为，以识别任何可疑或异常活动。例如，如果 API 突然在短时间内请求数千条记录，这可能表明 API 的业务逻辑遭到了破坏。现代 API 安全解决方案提供特定的威胁搜寻功能，支持安全团队尽早识别可能的威胁并采取响应措施。

什么是 WAAP?

Web 应用程序和 API 保护 (WAAP) 是市场调研公司 Gartner 对新兴 Web 和 API 保护解决方案划分行业覆盖范围时使用的一种分类。它是从 WAF 市场的早期行业覆盖范围发展而来的。随着 API 安全防护在战略上变得越来越重要，并且 WAF 平台以托管 SaaS 的形式迁移到云，WAAP 应运而生。

什么是 API 文档示例?

RESTful API（最常见的 Web API 类型）的 API 文档最常见的形式是基于 OpenAPI 规范的 Swagger 文件集合。理想情况下，API 文档由开发人员在设计或实施 API 时创建。但在现实中，API 文档经常失去时效，导致实际的 API 使用情况与文档不相符。为了解决此问题，有些 API 安全平台可以从实际 API 活动生成 Swagger 文件，突出文档记录与实际部署之间的差距，而这恰恰是任何 API 风险评估中不可或缺的部分。

有没有企业应遵循的 API 安全检查清单?

有效的 API 安全防护需要许多特定于企业的详细步骤和持续实践。不过，在提高 API 安全性时，安全团队可从如下 API 检查清单入手：

- 企业 API 安全方法是否包含持续发现企业范围 API 的机制?
- API 态势管理是否已纳入企业更广泛的安全和风险管理实践?
- 企业是否实施通用 API 安全方法，不会受限于特定的数据中心或云基础架构模式?
- 企业的安全方法能否为团队提供他们需要的业务上下文，帮助他们真正理解 API 活动和观察到的潜在风险?
- 企业是否设有 API 安全平台与其他相关业务流程（例如 SIEM/SOAR、威胁搜寻、文档、DevOps 工具等）之间的双向自动化策略?
- 企业是否采取了措施将非安全利益相关者（例如开发人员）纳入 API 安全防护工具和流程的考量?

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。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯