Akamai

电子书

API 安全的 8 大注意事项

塑造强大安全态势的关键因素

保护 API 真的那么复杂吗?

API 安全防护成为了许多 IT 主管首要关注的问题，这是有充分理由的。请参考以下这句话：

“随着 API 的爆炸式增长，它暴露出一个引人注目的攻击面，使得 API 安全防护问题继续成为安全主管心中的难题。”

—《API 安全防护的八个组成部分》，Forrester Research, Inc.，2023 年 9 月 28 日

促使 API 风险增长的因素

为应对不断增长的 API 风险，在开始实施有效的 API 安全防护之前，企业必须先了解以下关键内容：

API 是一个动态目标	
内部 API 意识	外部 API 暴露
快速发展的 DevOps 进程会不断创建和淘汰 API，使得企业无法获得全面的 API 清单	不成熟的 API 实践可能会导致意外地将敏感的 API 暴露给外部各方，包括许多影子 API

API 容易受到两种不同类型的威胁	
技术漏洞	误用和滥用
攻击者可以利用软件漏洞和错误配置，包括 OWASP API 安全十大漏洞	无论是否存在技术漏洞，都可能发生业务逻辑滥用和其他行为，如攻击性数据抓取

为解决复杂的 API 安全防护挑战，企业需要采取全面且深思熟虑的策略，其中包括以下几点：

结合最新的技术进步

打破企业中的壁垒

应对全面的 API 威胁态势

在为您的企业制定更先进的 API 安全防护策略时，可以遵循以下基本策略并规避相应的陷阱。

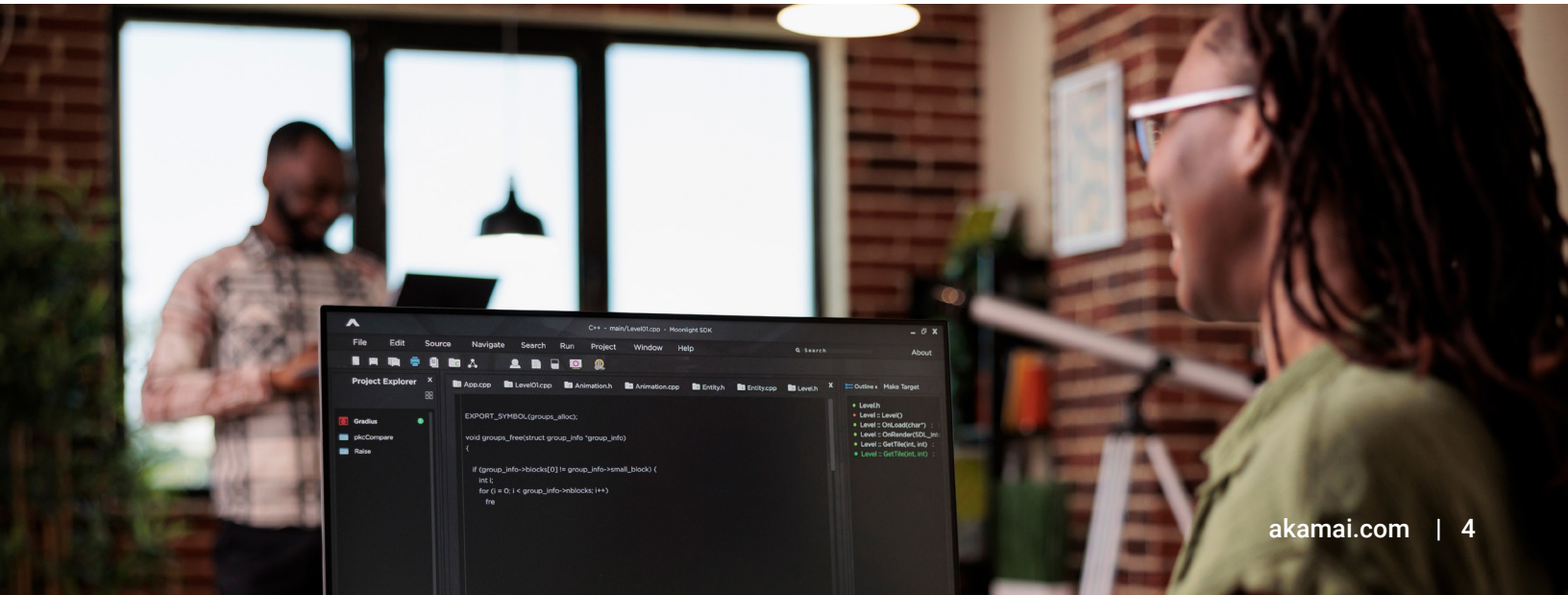
有效确保 API 安全的 8 大注意事项

1 坚持实现全面的 API 监测

无论怎么强调都不为过：如果您不知道自己拥有哪些 API，就无法对其进行保护。如果一个 API 长时间未被识别和监控，它就极有可能成为攻击者的目标。要实现全面的监测，最佳方法是确保您的 API 安全防护平台能够从各种来源收集信息。这些来源包括 API 网关、网络设备、微服务编排解决方案，以及云服务提供商等。具体而言，为了实现全面监测，API 安全防护解决方案应该具备以下能力：

时间	位置
• 持续发现 API • 监控各个 API 调用 • 记录短期会话活动 • 分析随时间而变化的 API 行为	• 检测整个企业中的 API • 发现旧 API • 找出影子 API

全面监测 API 有助于防止 API 数据泄露，尤其是在最新的数据泄露手段中，攻击者采用低速缓慢攻击从 API 中抓取数据。要防范这种新型攻击，首先要了解所有 API 的位置。



2 不要对云感到恐惧

Web 应用程序防火墙 (WAF) 利用签名技术来阻止未经授权的 API 进入您的企业。随着 API 攻击的不断演变，为了充分保护 API 免受各种潜在风险的侵害，您需要引入一个额外的防护层，利用行为分析技术来全面保护 API 的安全。当前至关重要的是对企业内部 API 的行为进行监控，而不仅仅是那些面向外部公开的 API。

为了充分发挥行为分析的效能，我们需要在云端对 API 流量进行深入分析。安全团队有时不愿意将涉及企业活动的敏感信息上传至云端。但是，对于众多企业生成的庞大 API 数据量，若没有云端所提供的规模和弹性，仅凭扩展的检测和响应技术来展开真正的行为分析，显然是不切实际的。

而且，由于安全团队的资源有限，漫长而复杂的产品部署也成为了前进道路上的主要障碍。随着 API 使用范围的不断扩大，安全团队必须迎头赶上，以应对这些挑战。因此，将云端纳入 API 安全防护策略是至关重要的。

3 坚持将业务情境置于策略的核心

发现 API 和识别安全风险只是缩小 API 攻击面的第一步。请思考以下三个问题：

1. 您如何确定特定合作伙伴的 API 凭据是否已遭到泄露？
2. 您如何判断企业间谍活动是否以数据抓取 API 的形式发生？
3. 您如何判断开票 API 是否被用户滥用，特别是当该用户试图通过枚举发票编号来窃取帐户数据时？

在第一个情境中，该活动似乎来自合法用户。因此，要有效检测恶意意图，唯一的方法就是密切关注 API 上预期行为的变化。第二个和第三个情境也是利用合法 API 访问模式进行未授权行为的例子。除了了解技术方面的信息外，深入理解业务情境对于这些情况也是至关重要的。

4 不要让数据变成一条单行道

有效的 API 安全防护策略的基本功能之一，就是将告警和事件发送至首选的安全监控工具和 IT 工作流工具。安全供应商以及负责发出告警的团队常犯一个错误：将安全告警和自动响应视为单向通信流。

与许多合法的业务流程类似，攻击可能会持续很长时间。为了充分发挥效能，针对 API 使用情况的行为分析必须至少持续 30 天。这为描绘基线预期行为提供了更完善且精准的画面。它还可以检测到在数天或数周内缓慢实施的攻击以及大量 API 会话。请考虑低于指定速率限制的低速缓慢数据抓取攻击：要察觉这样的行为，只能通过仔细审视历史行为并关注任何变化来实现。

没有具体支持细节的告警可以说弊大于利。提供具有详细原因和影响范围的告警，可以增强其实际操作性。然而，只有能够提供具有丰富上下文且可操作的告警，使接收者能够查询更广泛的数据集来分析事件，才能真正地制胜。随后，您可以使用 WAF 防护来立即阻止那些可能对您的业务构成潜在威胁的流量。

5 坚持优先考虑跨部门协作

为了从 API 安全防护中充分受益，我们需要在设计、开发和部署阶段主动采取措施，预防漏洞出现。为了高效地完成这项任务，需要与不同的团队协作。

要开始协作，首先要让 API 团队清楚地了解 API 在实际场景中是如何被使用（和滥用）的。随着时间的推移，这种透明度将有助于培养在 API 开发和部署流程中更早考虑安全防护的文化。此外，还要确保：

- 您的策略不仅具备核心安全功能，还具有一些非安全性方面的优势，这些优势有助于 API 团队更高效地开展工作。
- 即便是非安全领域的用户（如开发人员），也能轻松地查看和查询 API 清单和活动信息。
- 使用情境响应，例如集成到开发工具（如 Jira）中，主动为开发人员创建安全问题修复工单。

将 API 安全防护视为每个人的责任，并让安全团队以外的利益相关者能够轻松参与进来，以消除相互推诿的现象，并促使开发、运营和安全团队以互惠互利的方式进行合作。

6 不要忽视第三方 API

另一个需要避免的常见 API 安全防护策略陷阱是，认为您只需要关心自己的 API。尽管您期望自己购买的 WAF 或 API 网关能够统一管理整个 API 安全防护策略，但实际情况并不总是如您所愿。

例如，不要仅仅因为实施了集中式 API 网关策略，就以为影子 API 无法绕过核心 API 治理策略。如果您的业务依赖于任何第三方 API，那么您的网关将把这些 API 视为已通过身份验证，即使它们在连接到您的生态系统之前可能已被破坏。

您必须将 API 防护策略与您的主要 API 技术（例如 API 网关）相结合，同时从其他来源（例如网络设备、云平台和微服务编排工具）收集尽可能多的信息。这是纵览 API 攻击面全貌的唯一途径，也是确保安全防护策略在未来不受技术和基础架构变化影响的唯一方法。

7 不要被动回应，主动出击

尽管及时且高效地回应告警值得称赞，但如果您仅关注于在告警发生时如何减轻其影响，那么您将错失彻底预防告警出现的良机。正确的做法是，主动搜寻威胁。当您的 API 安全防护合作伙伴授权您执行数据查询时，您将有机会验证自己的假设，理解各元素之间的关系，并能够在潜在威胁升级为安全事件之前将其识别出来。比如，当您察觉到某个合作伙伴在 API 的使用上存在不当行为时，只需轻点几次鼠标，就可以快速查询到其他合作伙伴或供应商是否存在类似的行为。

所有 API 安全防护合作伙伴必须将历史数据存储在数据湖中，并确保您可以轻松访问这些数据，以便进行调查和识别潜在威胁。

理想情况下，您可以通过两种方式使用这些丰富的查询功能：

1. 简单直观的用户 Web 界面

2. 接入 API 安全防护提供商的一系列 API 接口，可用于开发更精密的工作流程

8 坚持将 API 安全防护视为一个持续的生命周期

要将 API 安全防护直接融入到业务中，最好的方式是执行 API 测试。通过在 API 生命周期中引入此工具，可以有效地减少将错误配置或易受攻击的 API 投放到生产环境的风险。在开发周期及早进行测试和修复，可以有效避免后期出现问题，从而充分节省时间并降低费用。

接下来，安全团队应该着手进行 API 防护工作，首先需要创建企业使用的 API 清单。随着 API 的不断新增和停用，安全团队必须时刻保持敏感应用程序和数据存储库中 API 接口的最新清单，这一点至关重要。通过持续进行有效的 API 检测，影子 API、恶意 API、被遗忘的 API、僵尸 API、孤立的 API 和已弃用的 API 等问题都将逐渐消失。

安全团队应具备足够的洞察力来识别和减轻新出现的 API 安全防护威胁。然而，在运行时环境中进行威胁检测也是必不可少的。业务逻辑滥用只会出现在生产环境的 API 中。通过将运行时行为与基线的正常使用模式进行比较，有助于揭示滥用行为。

最后，重要的是要在运行时期间的任何时候，阻止可能利用您的 API 的威胁。WAF 的自动拦截功能在这一步中发挥着至关重要的作用，因为仅对所有事件发出告警并不足以在宏观层面上全面保护您的企业。其他自动响应可以是多种多样的，且可根据需求进行定制，例如降低 API 网关的速率限制、创建 Jira 工单以便开发人员可以展开调查，或向安全团队发送电子邮件。只有在理解具体情境并且能够定制响应机制的情况下，才有可能对每个检测到的威胁做出适当的响应。

总结

坚持	禁忌
✔ 实现全面的 API 监测	✘ 不要对云感到恐惧
✔ 将业务情境置于策略的核心	✘ 不要让数据变成一条单行道
✔ 优先考虑跨部门协作	✘ 不要忽视第三方 API
✔ 将 API 安全防护视为一个持续的生命周期	✘ 不要被动回应，主动出击

立即开始

您是否已做好准备，迈出实施现代、系统化的 API 安全防护策略的第一步？

进一步了解 Akamai API Security。

只需几分钟，您就能开始使用 Akamai 基于云的策略。几个小时内，您将全面了解整个企业中 API 的使用情况，并深入洞悉业务逻辑与 API 之间的关系。