Akamai

API 发现的权威指南

目录

API 发现的重要性

无论您是刚开始关注 API 安全防护，还是希望进一步完善现有策略，发现并清点整个企业中的所有 API 都是必不可少的基本步骤。为什么？您的企业构建的每个应用程序，迁移到云端的每个工作负载，以及员工使用的每一种协作工具，都有 API 在后台负责交换数据，而且交换的往往是敏感数据。挑战在于，大多数企业尽管认识到拥有完整 API 清单的重要性，却无法真正地摸清其大部分的 API。

而无法识别 API，自然就无法确保其安全。

随着企业越来越以云为中心和不断提升数字化水平，其 API 资产的范围、规模和复杂性也随之不断扩展。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 已与第三方和开发者生态系统的应用程序、服务及系统建立起千丝万缕的连接。

随着您的 API 的范围、规模和复杂性不断增长，您将越来越难以获得有关以下方面的实时洞见：

- 您的 API 分布在各个业务部门的什么位置，多数情况下，这些业务部门都有自己的开发团队
- 您的 API 是如何配置的，它们的路由位置，以及是否具备适当的身份验证和授权控制
- 当您的 API 被调用并返回敏感数据时，谁可以访问这些数据

更为棘手的是，企业日积月累的大部分 API 都处于不受管、未识别以及通常未得到有效保护的状态。这些 API 包括休眠 API、影子 API 和僵尸 API，在很多情况下，它们会避开像 API 网关和 Web 应用程序防火墙 (WAF) 等常用工具的防御。这些工具确实提供了一些好处和基本保护，但在当今的 API 安全威胁形势下，我们需要更高的监测能力、实时保护和持续的测试，只有专业的 API 安全解决方案才能提供这些功能。

如果您能够发现所有的 API，就能为下一步的重要工作奠定基础，例如评估每个 API 的风险、了解企业的 API 安全态势，并利用所获得的洞见采取实时保护措施，防止攻击发生。在本白皮书中，我们将分享：

- 某些类型的 API 让安全团队难以捉摸的原因
- 有关 API 发现功能的详细信息，这些功能可以帮助您提高监测能力和预防遭受攻击

为什么 API 如此难以发现？

在生产环境中，经常会存在一些连运营团队或安全团队都不知道的不受管 API，这会导致企业面临一系列网络安全风险和运营难题。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，很容易受到恶意攻击。不仅如此，其他风险也异常之高。对 API 的攻击会损害企业的收入、恢复能力以及合规性。

以下是四种可能出现异常 API 的情况：

1. API 走捷径和进程故障

如果自行创建了 API 却没有告知合适人员，就会形成异常 API。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。

2. 旧 API 版本

在很多情况下，某个 API 的旧版本可能安全防护能力较差或者存在已知漏洞，但从未被删除。在软件更新期间，旧版不得不与新版本共存一段时间。但负责停用 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。一些 API 也可能已正式停用，但由于操作疏忽而仍在运行。这两种情况都会导致所谓的僵尸 API。

3. 继承的 API

因合并或收购而继承的 API 也经常会被忽略而成为影子 API。清单（若有）常常在系统集成的繁琐工作中丢失。由于小型企业的 API 环境通常杂乱无章且缺乏文档记录，因此频繁收购小型企业的大型企业尤其容易受到威胁。

4. 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 有时会在无人注意的情况下被激活。

什么是 API 发现？

API 发现既是一种流程，也是一组功能，可帮助企业识别、分类、管理和衡量其 API 的风险。如果执行得当，API 发现可以帮助企业：

- 减少 API 蔓延（即未经适当文档记录或监督的 API 数量迅速增长），并改善安全态势
- 更好地了解其当前的 API 安全状况，面向未来发展制定出明智的决策
- 监视和控制对这些 API 的访问，确保只有授权用户才能访问它们

利用关键 API 发现功能提高可见性和降低风险

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，无论配置或类型如何

检测

不受管的 API，如休眠 API 和僵尸 API

识别

被遗忘、被忽视或未知的影子域名

消除

监测能力缺口，发现潜在攻击路径

在评估新的 API 发现解决方案时，请记住以下功能——发现工具应包含所有这些功能。

发现所有 API 类型

API 发现工具必须能够识别各种配置或类型的 API，如 RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC 和 gRPC 等等。

精细的 API 清单

API 发现工具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。

检测难以发现的 API

不受管的 API 可能早在您的企业开展 API 安全防护计划之前就已经存在。您的 API 蔓延问题或许源于一个已不再隶属于您的企业的开发团队。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。因此，利用发现工具找到这些 API 至关重要。

发现影子 API 域名

除了影子 API 之外，您可能还有完全影子化的域名——也就是您对其一无所知的 API 域名。API 发现工具必须识别被遗忘、被忽视或可能构成安全风险的未知影子域名。

自动 API 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。

无需集成

API 发现工具应能够全面发现您的 API 资产，找到易受攻击的 API 和影子域名，而无需任何特殊集成或软件安装。这一点至关重要，可以防止因未能安装正确的代理或工具配置不当而产生的监测能力缺口。

限制定制开发

最后，API 发现工具的设计应能避免针对流量源进行定制开发的需求。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。

Akamai Security 如何帮助您发现所有 API

如果具备全面且持续的 API 发现能力，企业可以获得以下好处：

- 了解完整的 API 攻击面
- 降低 API 清单和文档更新的成本
- 提高对法规要求和内部政策的合规性

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。Akamai API Security 提供了这四个必不可少的模块，可保护 API 从开发到生产的整个生命周期。我们的 API Security 解决方案专门面向将 API 暴露给合作伙伴、供应商和用户的企业而构建，它可以发现您的 API，了解 API 的风险态势，分析 API 的行为，并阻止内部潜伏的威胁。

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 安全性服务简介

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：2024 年 10 月。