借助可靠的 API Security 推动亚太地区金融服务业发展

内容提要

根据国际货币基金组织的数据，2024 年亚太 (APAC) 地区的经济将继续大幅增长，增长率将达到 4.2%。在这样的增长发展形势下，特别是在金融服务业，应用程序编程接口 (API) 已成为行业数字化转型的核心驱动力。API 发挥着连接银行系统各个组件的技术桥梁作用，实现了数据和功能的无缝交换。API 彻底改变了提供金融服务的方式，为客户带来了诸多便利。

另一方面，API 使用量的快速增长也给企业带来了挑战，IDC 预测，到 2026 年，亚太地区的安全支出将达到 550 亿美元。随着金融机构通过 API 扩展其数字产品，他们也无意中暴露了众多安全漏洞。API 使用量的激增导致暴露给网络犯罪分子的潜在攻击面呈指数级增长。攻击者在认识到金融数据的内在价值后，已通过调整攻击手段来利用这些新发现的入侵点。

为了应对日益增长的威胁形势，金融机构被迫加大了网络安全措施方面的投资力度。金融机构不仅需要保护自己的系统，而且还需要保护客户的敏感数据和资产。因而，金融机构更加重视威胁检测、响应策略以及与业界同行和网络安全专家的合作，以抵御网络攻击所带来的风险。

由 API 驱动的亚太地区金融服务业数字化转型证明了该行业对满足客户不断变化的需求的适应能力和承诺。然而，随着这一转型的展开，该行业必须保持警惕，努力加强网络安全态势，解决安全漏洞，并确保数字创新的好处不会被无时不在的网络攻击威胁所掩盖。

API 的重要性日益凸显

亚太地区金融服务业正在经历一场数字化变革。API 已成为一股强大的推动力，为希望使用银行产品和服务的客户提供了卓越的便利性、速度和安全性。如今，客户使用移动设备就能进行各种金融活动，从查看账户余额和转账操作到申请贷款和管理投资，皆可轻松完成。这种便利性不仅为客户带来不一样的体验，还推动金融业进入数字化时代。API 已从简单的系统间通信工具演变成为互联网流量的支柱，支持广泛的应用程序和服务。

根据 Polaris Market Research 的报告，2021 年全球开放银行业务市场规模为 161.4 亿美元，预计到 2030 年将达到 1281.2 亿美元，预测期内复合年增长率为 26.8%。Polaris 的研究报告还重点指出亚太地区是预测期内增长最快的地区。亚太地区的金融服务业要想从开放银行业务的承诺中获益，就必须齐心协力应对 API 安全方面的挑战。

在亚太地区，新加坡的表现非常出色，新加坡金融管理局 (MAS) 发布了 API 指导手册。2018 年，新加坡金融管理局还牵头成立了 API Exchange (APIX)，这是一项与世界银行集团国际金融公司和东盟银行家协会共同发起的倡议。它是一个在线全球市场和沙盒平台，用于金融机构和金融技术机构之间的协作。

亚洲其他几个国家/地区长期以来一直致力于发展开放银行业务。印度一直在努力让金融普惠政策惠及该国大量无银行账户以及只能获得少部分银行服务的人口。

印度政府的早期举措之一是在 2016 年推出了统一支付接口，该接口允许公众使用 API 协议通过经授权的第三方访问银行账户并执行交易。2021 年，印度储备银行推出了账户聚合器，这是一个可创建同意管理器的框架，允许使用者以数字方式访问和控制其财务记录，并简化与金融服务提供商的数据共享流程。

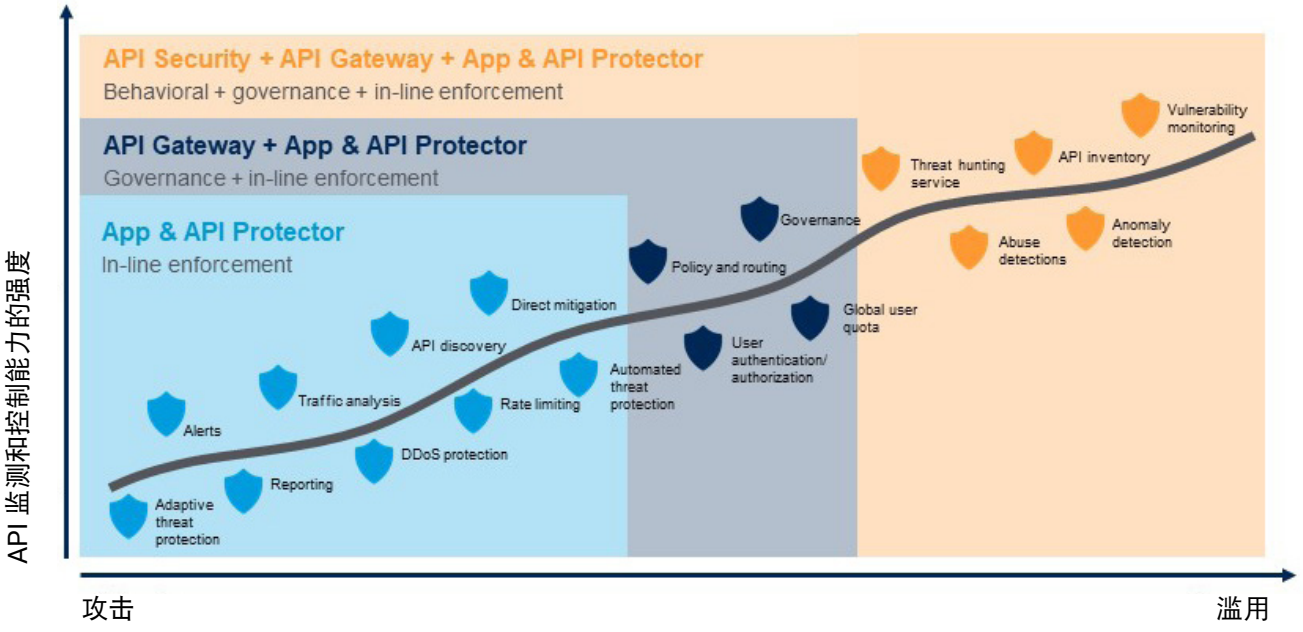
即使如此，亚太地区的金融服务业仍然是世界上受攻击最多的行业之一，从 2022 年第二季度到 2023 年第二季度，遭受的 Web 应用程序和 API 攻击数量增加了 36%，在 18 个月里遭受了 37 亿次攻击，次数之多，令人震惊。亚太地区拥有众多金融中心，遭受的 Web 应用程序和 API 攻击数量呈急剧上升态势。

亚太地区与 API 相关的威胁

亚太地区遭受的 Web 应用程序和 API 攻击数量急剧增加，从 2021 年到 2022 年，针对金融服务业的攻击增加了 248%。API 漏洞导致了多起备受关注的大规模数据泄露事件，包括澳大利亚的Optus 数据泄露事件和美国的 T-mobile API 数据泄露事件。这些事件凸显了拥有可靠的 API 安全解决方案的必要性，而这些解决方案的优势远不止于保护端点和检查凭据。

在本白皮书中，我们将探讨能够有效抵御这一高危攻击面并保护 API 的策略。此外，我们还将讨论主动式 API 安全方法如何确保合规性并提供数据保护。

API 攻击在不断演变



几种主要的 API 安全风险

API 很容易受到各种安全风险的影响，从而导致数据泄露、未经授权的访问和其他形式的滥用。这些主要 API 安全风险包括影子 API、易受攻击的 API、API 滥用、敏感信息过度共享以及撞库攻击。

- **影子 API。**很多金融机构都没有指定专门的人员或团队负责管理全部的 API。这种缺乏监管的局面导致了一种非常严重的安全隐患。发现整个企业内的 API 并对其进行编目对于管理和保护 API 至关重要。此外，消除开发人员与安全团队之间的安全隐患并在其环境中检测影子 API 也非常重要。借助持续发现功能，您可以随时了解新发现的 API 或现有 API 的变更情况，从而消除影子 API。

- **易受攻击的 API。**在发现 API 后，金融机构必须评估这些 API 的风险状况并识别其中是否存在安全漏洞，特别对于那些承载敏感数据的 API，更应进行评估。此步骤对于有效确定安全工作的优先顺序至关重要。

- **API 滥用。**随着数字化进程的加快，整个亚太地区的网络攻击数量持续上升。攻击者没完没了地攻击 API，因此需要强大的安全措施来阻止滥用和误用。

- **敏感信息过度共享。**现代应用程序常常过度共享敏感数据，从而形成新的攻击媒介。攻击者可以拦截流量并对敏感信息进行未经授权的访问。

- **撞库攻击。**攻击者以金融机构为目标，使用 API 自动进行撞库攻击。

API 安全防护挑战

未检测到和未报告的攻击

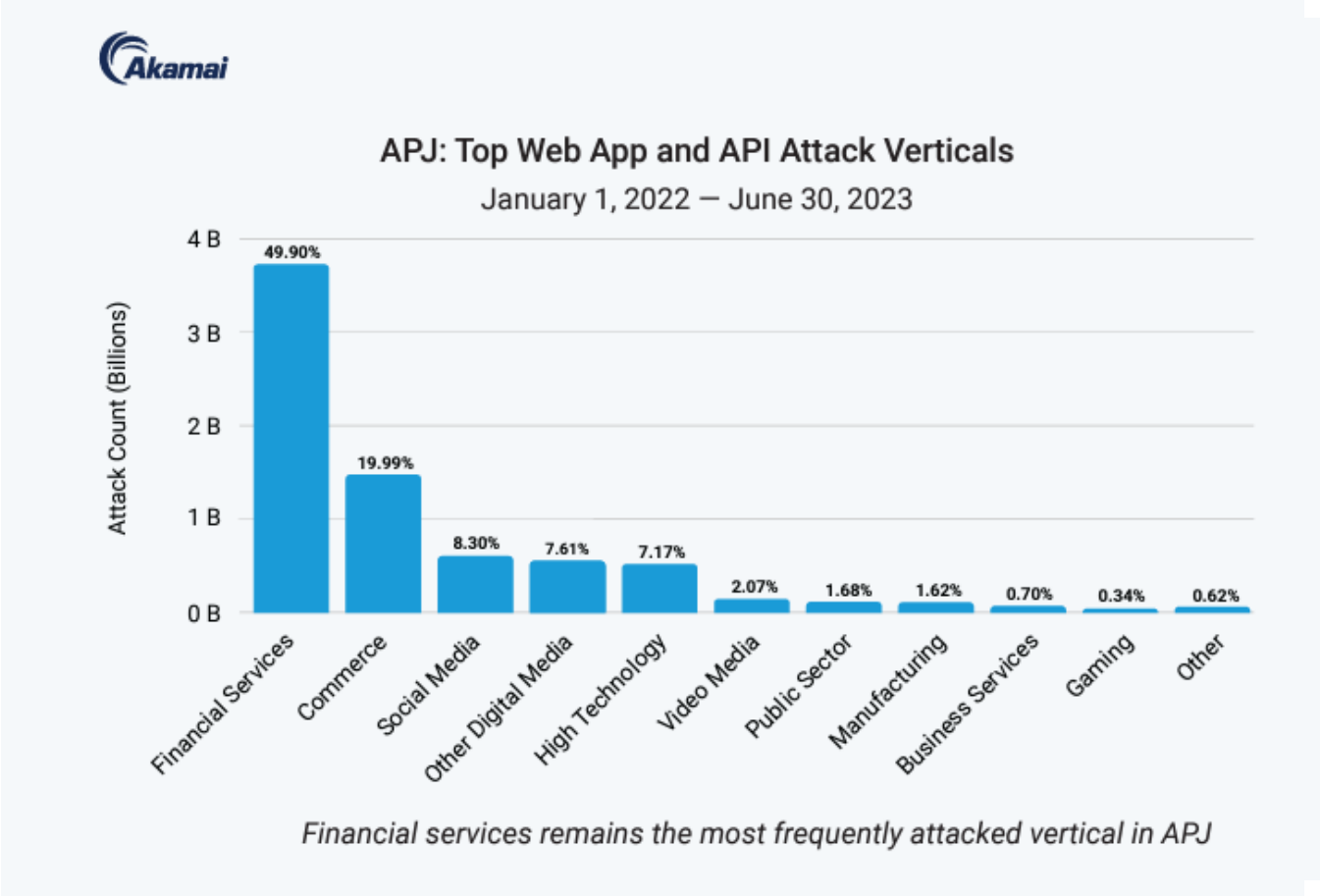
根据近期的一项 SANS 调查，API 清单仍然是金融机构面临的一个关键问题。金融机构甚至可能不了解其基础架构内的所有 API，因而形成管理和安全防护盲点。缺乏监测能力可能是导致 API 攻击常常未检测到和未报告的关键因素之一。保护 API 的第一步是发现所有 API 并对其进行编目。

破坏性 API 攻击的影响

Web 应用程序和 API 的可用性中断可能会大大影响客户满意度和品牌忠诚度。随着越来越多地采用数字化优先方法，API 对于金融机构的成功变得更加重要，而在当今金融科技公司和传统银行广泛接受开放式银行业务的背景下更是如此。

API 流量快速增长

金融业 API 流量快速增长，流量增长达三位数。这种增长形势对安全控制措施构成了挑战，只有选对安全控制措施，才能抵御不断演变的 API 威胁。



Financial services remains the most frequently attacked vertical in APJ

法规和安全防护

利用 API 和其他创新技术的金融机构发现自己需要实现公共政策和金融稳定目标。在亚太地区金融监管机构的多元化格局中，存在着提高客户成果的共同承诺。首要目标是扩大金融选择范围，促进竞争和可及性，以及促进金融普惠的落实。整个亚太地区的监管机构正在竭力扩大金融服务范围，让个人和企业从中受益。

根据世界银行的数据，全球有 17 亿成年人没有银行账户，这一数字令人震惊。值得注意的是，无银行账户的人口比例最大的三个国家都位于亚洲，其中中国占 13%（约 2.25 亿人），印度占 11%（1.9 亿人），印度尼西亚占 6%（9,600 万人）。在亚太地区，这些无银行账户和只能获得少部分银行服务的个人和企业形成了一个巨大的蓝海市场，估计规模在 550 亿美元至 1150 亿美元之间。

法规在 API 安全防护中的作用

修订后的支付服务指令 (PSD2) 等法规要求传统机构与外部实体共享数据，从而提高透明度。这些法规旨在保护最终用户的数据、隐私和安全。金融机构必须在持续创新同时遵守这些法规。

虽然这些法规鼓励数据共享，但同时也规定了企业必须如何存储和保护数据以及如何确保数据访问安全性。Akamai 解决方案不仅有助于金融机构遵守这些法规，而且不会妨碍其创新工作。

构建稳健 API 安全策略的 6 个步骤

通过保护端点和检查凭据来防范基于 API 的攻击显然不够。可靠的 API 安全策略必须包括以下六个步骤。

1.与合作伙伴协作

金融机构及其安全合作伙伴必须密切合作，协调人员、流程和技术，以建立针对 API 安全风险的强大防御措施。这种协作需要开发团队、网络和安全运营团队、身份团队、风险管理师、安全架构师以及法律/合规团队的共同参与。

2.API 的发现和编目

保护 API 的第一步是发现整个企业内的 API 并对其进行编目。通过此过程，安全工程师能够了解攻击面的范围以及敏感信息的潜在暴露情况。

3.测试漏洞并评估风险

一旦发现 API，金融机构必须执行漏洞测试和风险评估，及时识别和解决漏洞。此流程应当集成到 API 开发和升级周期之中，以确保持续的安全性。

4.实施行为检测

API 保护是整个应用程序安全框架的关键组成部分。行为检测是防止易受攻击的 API 被利用的关键策略。此方法需要持续监控和分析 API 行为以识别潜在威胁。

5.优先考虑“OWASP 十大漏洞”控制措施

金融机构应当优先考虑开放全球应用程序安全项目 (OWASP) 十大 API 安全风险，以确保全面保护。这些控制措施涵盖了影响 API 的关键漏洞和攻击媒介。

OWASP API Top 10 coverage by Akamai

- ☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- ☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- ☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- ☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- ☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- ☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- ☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- ☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- ☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- ☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

6. 向同行学习

金融机构应当向同行学习并分享最佳实践。金融服务信息共享和分析中心 (FS-ISAC) 的成员可以利用其情报平台、资源和值得信赖的点对点专家网络来预测、抵御和应对网络威胁。清楚地了解其他企业如何应对 API 安全挑战有助于增强整个行业的安全措施。

结论

在这个快速数字化转型和广泛采用 API 的时代，实现 API 的设计宗旨——也就是促进跨广泛软件、设备和数据源的灵活、快速且经济高效的集成，同时保护 API 的安全性对于金融机构而言至关重要。尽管如此，API 安全仍然是一项需要兼顾各方的复杂任务，涉及各种特性、功能和业务需求。忽视 API 安全可能会导致严重后果，包括网络攻击、数据泄露、违规以及机构声誉受损。

我们的数据表明，API 功能是攻击者的首要目标之一，他们会不断更新并改变攻击方法。因此，API 安全防护必须转移至边缘，远离您的基础架构，更靠近客户与您的数据和应用程序交互的数字化接触点。这一战略调整对于确保为您的数字资产提供可靠保护至关重要。

访问 akamai.com/finserv，详细了解 Akamai 在金融服务方面的优势

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：2024 年 2 月

扫码关注，获取最新CDN前沿资讯