

面向 IBM API Connect 和 DataPower 的集成 API 安全防护和治理能力

API 的前景与挑战

一直以来，API 在推动数字化转型方面发挥着关键作用，帮助各行各业的企业打造新的服务和业务模式，推动业务增长。但是，随着 API 数量的激增，API 的风险也随之增大。

- 业务和工程负责人在企业内快速地推进了 API 的使用和集成，然而，如何有效地管理 API 依然是个难题。
- 企业专注于比拼新应用程序及 AI 增强型服务的构建和发布速度，导致底层 API 常常包含错误配置、代码编写错误和业务逻辑问题。
- 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（通常是敏感数据）的无缝交换，而攻击者对此一清二楚。

因此，API 已成为一种具有高风险的主要攻击媒介。对 API 的攻击会损害企业的收入、恢复能力以及合规性。

为了应对这种挑战，企业必须采用全生命周期方法来实现治理和安全防护，涵盖从设计、开发、测试、部署、运营到修复的每个环节。借助 Akamai API Security 与 IBM 的技术，企业可以自信地快速开发、部署和管理 API，从而能够提前响应业务需求，支持业务扩展。

挑战

-  维护整个资产的 API 清单和发现未知 API
-  识别不合规、错误配置或易受攻击的 API
-  检测并阻止 API 滥用或不当使用，包括业务逻辑攻击
-  构建安全、一致的 API，而无需牺牲速度或敏捷性
-  建立 API 安全性和治理计划的调整与监督措施

Akamai 和 IBM 如何帮助客户

发现您的 API 资产

您无法保护看不见的资产。借助 Akamai API Security，您可以自动发现 API、域名和问题，从而生成可靠的 API 清单，全面了解您的 API 资产——通常，企业找到的 API 数量往往远多于他们自认为拥有或预期的数量。您还可以轻松找到可利用的情报（如泄露的信息），以了解对手可利用的攻击路径，并与 API 网关和管理平台相邻的最常见基础架构要素进行无缝集成，以确保在整个企业内实现安全数据的一致共享。

增强您的安全和治理态势

在使用 Akamai API Security 进行 API 治理时，扩展您的运营并实施最佳实践：

- 通过完整的业务情境了解您生态系统中的每个 API，并遵循 API 管理最佳实践
- 简化开发团队与安全团队之间的沟通
- 从错误配置到不符合策略的 API，发现各种漏洞
- 保护敏感数据并主动监控相关变化以降低 API 方面的风险



通过运行时保护来阻止 API 滥用和攻击

通过实时流量分析、带外监控、内联修复选项以及工作流集成，检测并阻止从边缘到核心的 API 攻击（包括数据泄露、数据篡改、数据策略违规、可疑行为等），从而提高安全运营中心 (SOC) 的有效性。

通过主动测试更快地交付安全 API

无缝地将 API 安全测试集成到 API 开发的每个阶段，并在 API 进入生产环境之前发现漏洞、错误配置和合规性问题。借助主动测试，DevSecOps 人员可以按需执行一整套 200 多项侧重于 API 的安全测试，或者将这些测试整合到公司的 CI/CD 流程之中。主动测试会根据对应用程序底层业务逻辑的理解来查找和测试每个 API，这使开发人员能够发现其他测试工具可能忽略的复杂漏洞。

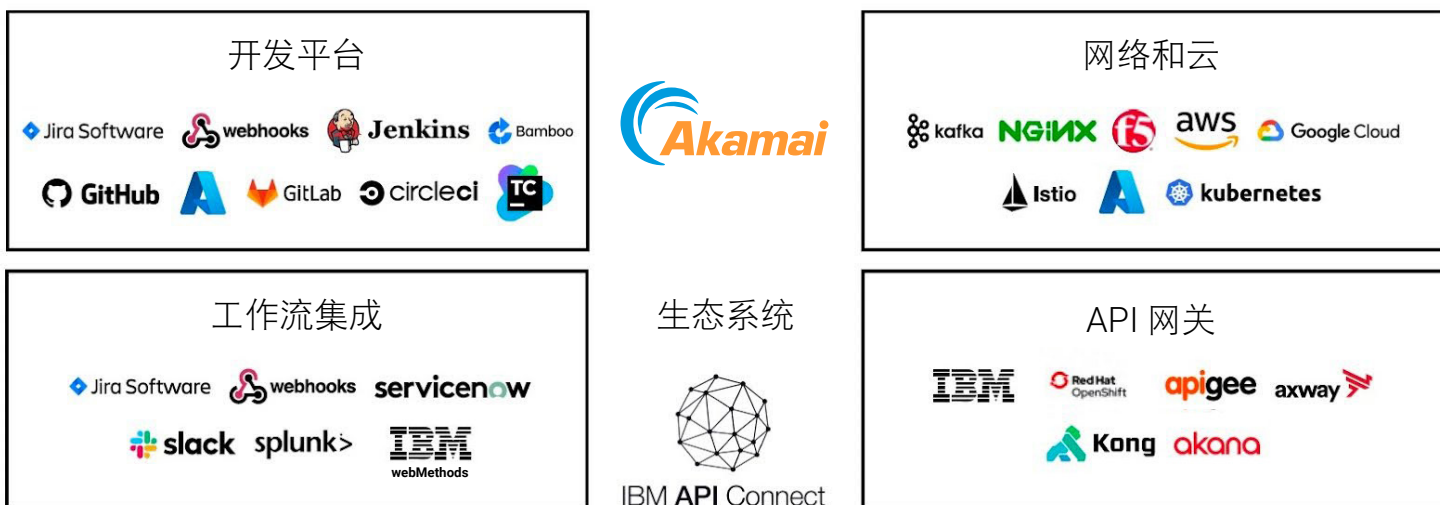
Akamai 如何通过高效的集成，助力 IBM 用户获得监测能力和保护

Akamai API Security 可以跨多个云平台并通过各种部署选项与 API Connect 和 DataPower 进行集成。此外，当 API Connect 管理 DataPower 时，会在各系统中进行单方面配置更改，从而提高运营效率，同时降低未经授权和不合规开发活动的风险。

无缝攻击定向和响应

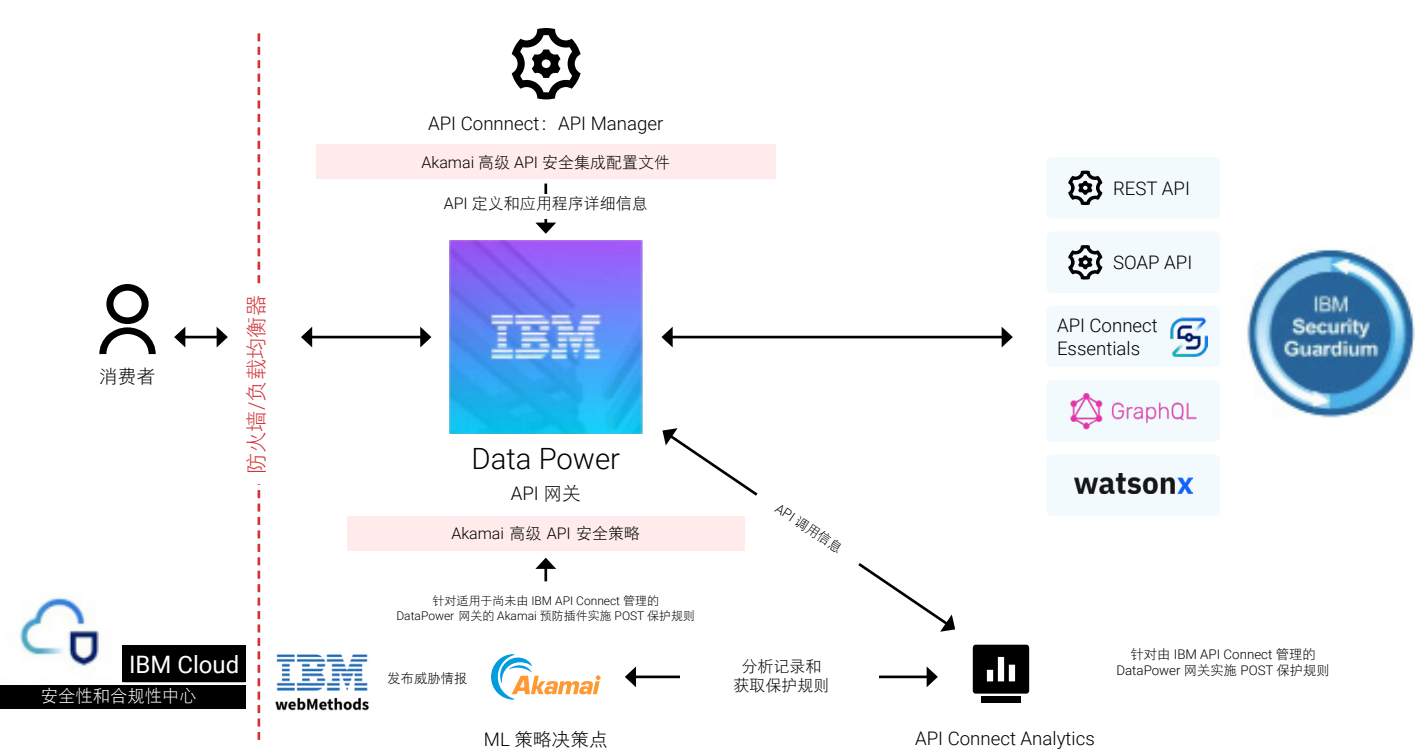
此外，通过与 Akamai API Security 解决方案进行集成，IBM DataPower 客户可以体验近乎实时的威胁检测和拦截，而不会遇到影响性能和延迟的问题，也无需在 DataPower 网关上安装任何其他插件。

IBM API Connect 可以根据 Akamai API Security 授权策略评估对资源的访问请求，并在 IBM DataPower 集群中实施拦截规则，从而将修复时间从几天缩短为几分钟或几秒钟。



将 IBM webMethods 与 Akamai API Security 的强大功能相结合，以实现出色的 API 管理和保护。本次合作提供了一个将 Akamai 先进的 API 发现功能与 IBM webMethods 强大的治理与实时数据集成功能相结合的全面解决方案。全面了解并控制您的 API 以确保安全性和合规性。此集成不仅能够增强防御能力，还提高了效率，让您的企业可以快速、安全地应对不断变化的市场需求。

最后，IBM DataPower 客户可以利用 Akamai eBPF Red Hat OpenShift 集成来发现尚未由 API Connect 进行管理或未由 DataPower 进行代理的 API，从而能够发现并保护处理高风险交易和机密数据的 API。这些功能从本地扩展到云和混合配置，并支持 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP)。



后续步骤

API 是企业满足客户需求、创造收入以及在瞬息万变的数字经济中保持竞争力的关键驱动力。但是，API 的持续增长、与数据相伴以及存在无数漏洞等因素，使得 API 成为攻击者眼中诱人的目标。随着 API 安全事件的稳步增加，企业必须具备查看、保护和测试整个企业内每个 API 的能力。IBM 与 Akamai 的强强联手可以让企业放心、安全地大规模构建、维护和使用 API。



扫码关注 - 获取最新云计算、云安全与CDN前沿资讯

预约定制化 Akamai API Security 演示，了解我们如何为您提供帮助。您还可以与 IBM 联系人进行沟通，以了解更多信息。