CLOUDFLARE

API 安全和管理的现状

应用程序编程接口 (API) 驱动全新的应用体验——从跟踪健康数据到个性化在线游戏。它们还支持着无数商业优势：客户分析、SaaS 集成、生成式 AI 能力等等。

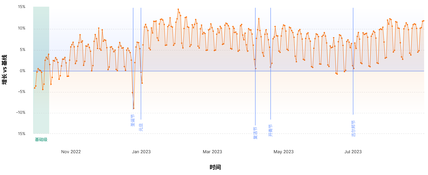
同时，API 难以管理并不断受到攻击。现在 API 流量已经**占到了总体动态互联网流量的一半以上 (57%)***，让我们看一下 API 流量的安全和管理趋势。

30.7%

与通过客户提供的会话标识符相比，通过机器学习发现的 API REST 端点多出近 31%

以 API 为中心的世界

总体而言，2023 年全球 API 流量持续稳定增长。



API 流量占自身总体 Web 流量比例最高的 10 个行业：

1. IoT 社区平台
2. 轨道、公交和出租车
3. 法律服务
4. 多媒体、游戏和图形软件
5. 物流、供应链与运输
6. 消费电子产品
7. 金融软件
8. 安全和调查
9. 银行、金融服务与保险
10. 医疗设备

未受保护的 API

缺乏全面 API 清单的组织面临“影子 API”风险 — 即隐藏的攻击面：

59.2%

向错误的人提供 API “型”访问权限可导致安全风险。许多 (59.2%) 组织向至少一半的 API 提供“型”访问权限（即推送更新的能力）。

15000+

超过 15000 个使用 Cloudflare 的账号拥有仅通过机器学习方法发现的 API 端点。

常见 API 漏洞

随着 API 流量、错误和攻击增长，市场对 API 安全和管理的需求已大幅飙升

API 面临的头号威胁
HTTP 异常 — API 最常面临的威胁 — 是恶意 API 请求的常见信号。

头号 API 流量错误
超过一半 (51.6%) 来自 API 源的流量错误包含 **‘429’ 错误代码：“请求过多”**。

头号缓解方法
三分之一的 API 缓解措施包括阻止分布式拒绝服务 (DDoS) 攻击

保护 API 与 Web 应用的挑战对比

VS

Web 应用

- 对最终用户**可见**
- 由**最终用户**通过 Web 浏览器**访问**
- **可视化数据**—— 数据来自后端（使用 HTML、CSS 和 JavaScript），提供不同的用户交互。
- 一般通过 **“负面安全”**模式来保护，即阻止已知的恶意流量。

API

- 对应用程序用户**可见**
- 让**系统和应用**交换数据
- **传输数据** ——通过使用预定义的格式（最常见的是 RESTful JSON、gRPC、XML、GraphQL）访问服务器和应用程序。
- 通过 **“正面安全”** 模式提供更有效的保护，仅允许通过验证和身份认证的流量。

保护 API 的三种重要方法

采用 “正面安全”模式 vs 采用 “负面安全”模式

正面安全模式中，您仅接受 “已知良好” API 流量（根据 API schema 定义）。这比负面安全更有效，因为负面安全只专注于限制 “已知不良” 的 API 流量。

应用机器学习以释放资源并降低成本

机器学习能够发现所有 API 流量（包括攻击变种），区分合法的流量高峰和恶意的机器人流量，并处理其他资源密集型的 API 管理任务。

统一应用开发、可见性、性能和安全性

全球连通云 — 在网络、云、应用和用户之间实现任意对任意连接 — 提供应用开发和 API 纵深防御服务之间的关键连接纽带。

CLOUDFLARE

想要了解更多？

欢迎阅读 Cloudflare《2024 年 API 安全和管理报告》全文

阅读报告

** 本信息图表中的数据发现基于 Cloudflare 全球网络（包括 Cloudflare 的 Web 应用防火墙、DDoS 防护、机器人管理和 API 网关服务）在 2022 年 10 月 1 日至 2023 年 9 月 31 日期间观察到的汇总流量模式。