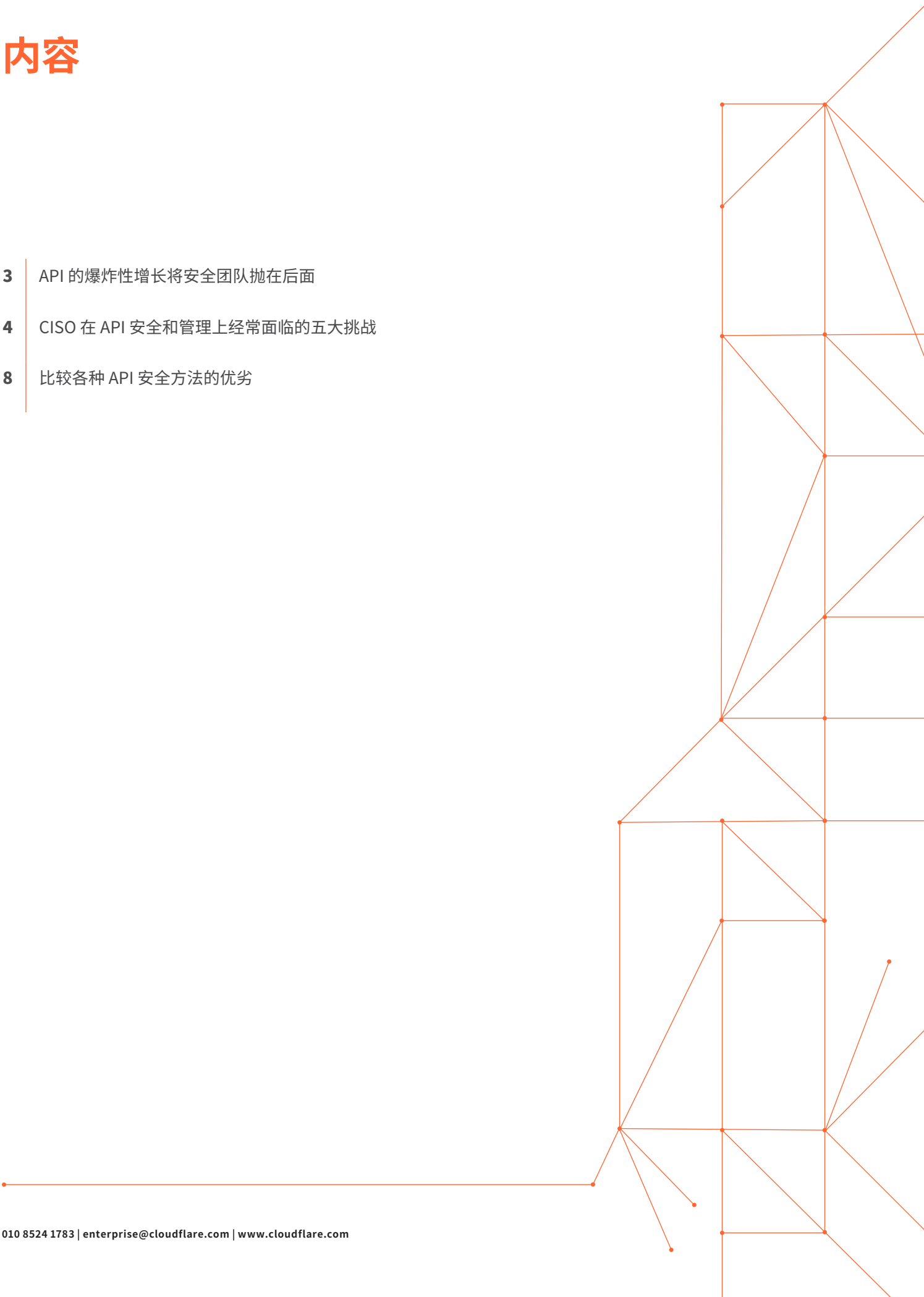
CLOUDFLARE

电子书

CISO 的 API 安全指南

防止数据泄露、影子 API、滥用和其他常见挑战的策略

内容



API 的爆炸性增长将安全团队抛在后面

API 带来了令人兴奋的商业机会，可以更快地交付产品并改善客户体验。现在，安全领导人必须设法在不减慢创新的情况下确保 Web 应用和 API 的安全。

近年来，API 造成的数据入侵和泄露已经成为新闻头条——包括印度的 JustDial，社交媒体领域的 LinkedIn 和 Twitter，甚至 T-Mobile。

为什么会这样呢？不幸的是，攻击者通常认为 API 比组织的核心 Web 应用程序更容易攻击。如果没有适当的 API 管理，这种假设通常是正确的。

现代 CISO 意识到需要整合 Web 应用程序和 API 安全。他们需要保护客户的敏感数据，同时支持跨 Web 应用程序和 API 资产的业务运营。

毕竟，这事关客户的信任。

58%[1]

的动态 HTTP 流量通过 API。

Gartner® 预测，到 2025 年，

少于 50%[2]

的企业 API 将得到管理，原因是 API 的爆炸性增长超过了 API 管理工具的能力。

API安全成熟度曲线 —— 各阶段和下一步

1

第一阶段：
从 API 安全性开始

首先识别组织中使用的所有 API。

发现 API 的多种方法：
使用 API 发现工具，查看技术文档和协议，与开发人员交流并监控您的 Web 流量。

2

第二阶段：
使用自行开发的流程

您的工具能否满足领导层的可见性和合规需求，以及安全团队的使用需求？

更好地整合工具以减少数据入侵、数据泄露、影子 API 以及可用性和韧性风险。

3

第三阶段：
整合安全工具

如果您正在寻找易于部署、专注于运行时且对安全团队具有成本效益的解决方案，就应该考虑 Web 应用程序和 API 保护（WAAP）。

1 2022 年度 Cloudflare Radar 分析

2 Gartner®“API 保护创新洞察”，分析师 Dionisio Zumerle、Jeremy D'Hoinne、Mark O'Neill，2022 年 10 月 10 日。
GARTNER 是 Gartner, Inc. 和/或其附属公司在美国和国际上的注册商标和服务标志，在此经许可使用。保留一切权利。

CISO 在 API 安全和管理上面临五大挑战

挑战一		**影子 API**：现代 CISO 需要掌握生产中所有的 API ——无论是在 IT 部门以外开发的 API 还是仍在使用的传统 API。每个组织的 API 开发速度有增无减。
挑战二		**安全漏洞**：现代 CISO 需要确保其组织的 API 都要求适当的身份验证和授权。迄今为止，许多 API 访问控制措施已经被攻击者轻易地利用。
挑战三		**数据泄露**：对于通过 API 交换的敏感数据，现代 CISO 需要拥有安全可见性和控制，无论是 PII/PCI/PHI 数据、凭据或令牌。
挑战四		**API 滥用**：现代 CISO 认识到，如果 API 被滥用流量淹没，可能会对您的组织造成与威胁行为利用安全漏洞一样的危害。
挑战五		**合规**：现代 CISO 必须确保他们面向客户的 API 符合行业和组织标准——无论是 PCI、HIPAA、GDPR、FFIEC 还是 FCA。

API 安全是否不同于 Web 应用程序安全?

是的。由于如下特征，API 是一种独特的攻击面：

- API 在系统之间交换数据。最终用户通过 Web 浏览器访问 Web 应用程序
- API 使用不同的格式（通常是 JSON）来传输数据。Web 应用接受用户输入并从后端可视化数据（使用 HTML、CSS 和 JavaScript）
- API 直接访问后端系统，通常作为现代 Web 应用程序和其后端数据库和服务器之间的中介
- 成功的 API 交易假设为合法访问
- 由于对最终用户不可见，API 容易被忽视

与 Web 应用程序安全相比，API 安全需要有意义的业务上下文、不同的发现方法、更深入的访问验证控制和智能的滥用保护。

即使在重叠的漏洞类别（例如注入攻击和访问风险）中，API 安全的检测方法也不同于 Web 应用程序安全。例如，在代表调用方执行任何工作之前，每个 API 操作都必须验证调用方的身份和权限。

挑战一：影子 API

领导者的安全考虑

影子 API 是现代组织中一个日益令人担忧的问题。大多数 IT 和安全人员找到和管理 API 的速度落后于开发人员构建 API 的速度。

当前许多用于跟踪 API 的流程存在问题，使用手动方法，安全团队需要不断地向开发团队追问更新情况。

可以向您的团队提出的一些问题：

- 今天如何发现和管理公共 API?

团队的安全考虑

在您的环境中定期执行 API 发现，就像您对 IT设备和应用程序一样。

向领导报告的有用指标包括：

- 确定哪些组具有最多影子 API 而造成更大风险，因而需要优先开展流程改进。

挑战二：安全漏洞

领导者的安全考虑

安全团队面临着比以往更大的压力，要防止组织因安全漏洞而成为新闻头条。攻击者已经开始利用许多 API 中的弱身份验证和授权措施。

可以向您的团队提出的一些问题：

- 如何在 API 中进行身份验证和授权?
- 您的 API 是否遵循一致的规范和格式?

团队的安全考虑

确保您的 API 对每个 API 操作都验证身份和授权令牌。

向领导报告的有用指标包括：

- API 资产清单——突出显示那些携带敏感数据、不符合法规或使用弱认证或授权方法的 API 资产

“随着我们的 Web 资产数量增加，我们面临着 DDoS 攻击、数据爬虫和繁琐的证书管理等问题。我们希望获得一个安全层，能够在不增加显著开销的情况下保护我们的 Web 资产和 API。”

Marut Singh
CTO，CARS24

挑战三：数据泄露

领导者的安全考虑

API 通常会携带敏感数据。作为 CISO，您希望确保 API 不会暴露错误的敏感数据，并且 API 在强加密下传输数据。

可以向您的团队提出的一些问题：

- 您的数据丢失预防 (DLP) 程序是否包括通过 API 的数据丢失？
- 您是否了解最新的法律和行业特定的数据安全要求？
- 您的数据在静止和传输过程中是否安全？您是否为您的行业和司法管辖区使用了适当的加密标准？

团队的安全考虑

- 检查在 API 请求中使用的暴露/泄漏凭据
- 在 API 请求和响应中扫描个人身份信息(PII)、信用卡数据和个人医疗保健信息

挑战四：API 滥用

领导者的安全考虑

很多情况下，API 并不对客户端/用户请求的资源大小或数量施加任何限制。

这不仅会影响 API 服务器的性能，导致拒绝服务 (DoS)，而且还会为暴力破解等身份验证缺陷敞开大门。

就像对待 Web 应用程序一样，监视 API 流量对于确保业务产品和服务对客户可用至关重要。

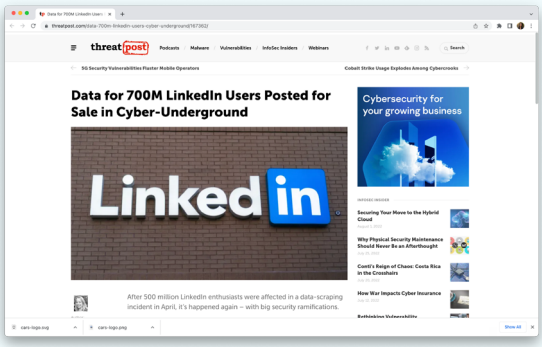
可以向您的团队提出的一些问题：

- 您的工具是否可以限制滥用的 API 流量？
- 你怎么知道每个 API 的适当流量限制是多少，任何响应中有多少个资源？

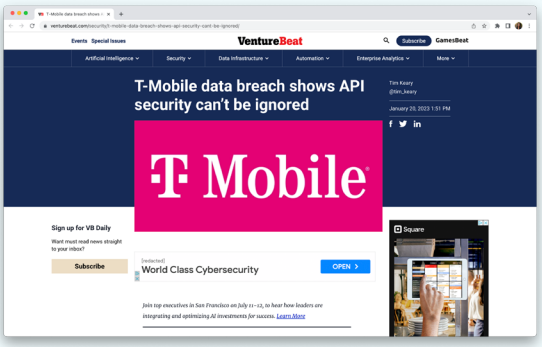
团队的安全考虑

根据每个端点观察到的流量模式，在您的 API 上部署智能速率限制。

API 安全漏洞



文章：LinkedIn —— 7 亿用户数据被爬取



文章：在过去的几年中，T-Mobile 的 API 漏洞受到利用

挑战五：合规

领导者的安全考虑

在许多行业和地区，数据隐私和本地化法规不断变化，如果没有一致的流程和工具，几乎不可能实现合规。

安全工具可以识别敏感数据，将相关信息推送到您的管理解决方案中，并与您的 SIEM/SOAR 集成，以协调适当的响应。

可以向您的团队提出的一些问题：

- 您的安全工具是否可以帮助您识别 API 中出现的相关敏感数据？
- 您是否可以将 API 安全情报与其他安全工具集成？

团队的安全考虑

在 API 请求和响应中扫描个人身份信息(PII)、信用卡数据和个人医疗保健信息。

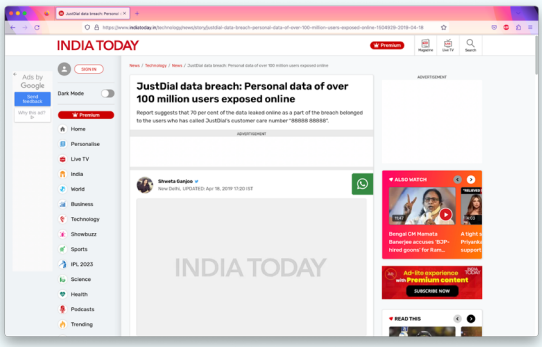
保留有关 API 使用情况、安全警报和采取的响应操作的审计日志。

向领导报告的有用指标包括：

- 在您的 API 中，每种适用的数据类型出现的实例数量。

API 安全漏洞

文章：Twitter 的 API 暴露过多信息



文章：JustDial 的传统 API 暴露客户数据

比较各种 API 安全方法的优劣

在现代组织中，管理和保护所有 API 增长有多种方式 —— 全生命周期 API 管理、API 可观察性和全面的 Web 应用程序保护。

为了在不抑制创新的情况下实现公共 API 的全面安全和性能，可以考虑 Web 应用程序和 API 保护解决方案采取的方法，例如 Cloudflare API Gateway。

API 可观察性工具	Web 应用程序和 API 保护 (WAAP)	全生命周期 API 管理
用例： 预生产环境中的 API • 需要另一个工具来生成 API 流量 • 无法保护 API 免受滥用/攻击；需要连接到 Web 应用程序防火墙 (WAF) 以阻止	**用例：** 生产环境中的 API，实时监控，防御滥用、零日漏洞利用和攻击者 • 提供实时 API 保护（相比 API 安全点解决方案） • 比全生命周期管理解决方案更易于部署和管理 • 与您的 API 集成，与云服务提供商、API 结构和开发语言无关	**用例：** 受高度监管行业中和传统 API 标准中的 API • 这些工具通常专注于 API 管理，但在安全方面不够充分 • 这些工具对开发人员来说集成更为麻烦

Web 应用程序和 API 保护解决方案的主要功能

- 影子 API 发现
- 集中管理 API 并监控使用情况
- 身份验证（mTLS 和 JSON 令牌）
- 针对常见行业和法律要求的敏感数据检测
- 传输中数据加密
- 积极的实时阻止和流量接受安全模型
- 来自实时流量分析的威胁情报
- 机器学习驱动的滥用和漏洞利用保护
- 优化边缘网络以不间断地服务 API 流量

Cloudflare 应用安全产品组合

Cloudflare 确保应用和 API 安全、高效，阻止 DDoS 攻击，拦截机器人，检测异常和恶意负载，并监控浏览器供应链攻击。

保护 API 而不抑制创新

联系我们

CLOUDFLARE

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-4431.2023APR06