Cloudflare API Shield

管理和保护驱动业务的 API

现代 API 面临的挑战

成为攻击者的目标

API 驱动世界运转。Cloudflare 网络上 58% 的动态 HTTP 流量与 API 相关。

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。

安全和 IT 团队需要保护客户的敏感数据，同时支持跨 Web 应用和 API 资产的业务运营。

毕竟，这事关客户的信任。

Cloudflare API Shield

通过在 Cloudflare 边缘整合 Web 应用和 API 保护，客户能够发现、保护和简化其公共 API 的安全和管理。

API Shield 是 Cloudflare 应用安全产品组合的一部分，这个产品组合还可以拦截机器人、挫败 DDoS 攻击、阻止应用攻击和监控供应链攻击。

影子 API 风险

开发团队往往在未通知 IT 的情况下发布新的 API，因此这些 API 在没有管理或安全保障的情况下运作。

身份验证、数据丢失和滥用担忧

这些 API 一经发现，就必须通过身份验证、模式验证、API 滥用保护和数据泄露检测来防止攻击和滥用。

API 性能监控

鉴于 API 驱动着业务，一旦 API 受到监控和保护，企业必须密切关注其性能：了解每个端点的请求量、错误率、延迟。

Cloudflare API Shield

管理和保护驱动业务的 API

主要功能	
API 管理	
发现和模式学习	通过机器学习驱动和启发式的模型，发现活跃使用中的 API 端点及其相关模式。
序列与性能分析	发现 API 调用行为的最重要序列，并分析 API 端点性能（例如请求数、延迟、错误率、响应大小等）。
开发人员门户和管理	使用 Cloudflare Pages 管理交互式 API 文档，并将其托管在您的域上。
API 安全	
身份验证和校验	使用 mTLS 证书、JSON Web 令牌 (JWT)、API 密钥和 OAuth 2.0 令牌对 API 流量进行身份验证和检查，以阻止来自非法客户端的请求。
模式验证	使用 API 模式接受有效的 API 请求，并阻止格式错误的请求和 HTTP 异常。这补充了 Cloudflare WAF 的负向安全模型，实现全面的安全防护。
REST 和 GraphQL 滥用保护	通过基于每个端点会话的速率限制建议，阻止容量耗尽型和序列滥用。将拒绝服务 (DoS) 保护扩展到 GraphQL 端点。
敏感数据检测	在源服务器的 API 响应中检测敏感数据，并按端点发出警报。
集成平台	Cloudflare 应用安全通过单一集成控制台进行管理，提供事件分类、规则和分析功能。

产品优势

- 最小化攻击面风险，降低网络安全风险
- 提高 API 性能
- 减轻运营负担：时间和成本
- 在统一的性能和安全平台上整合 Web 应用和 API

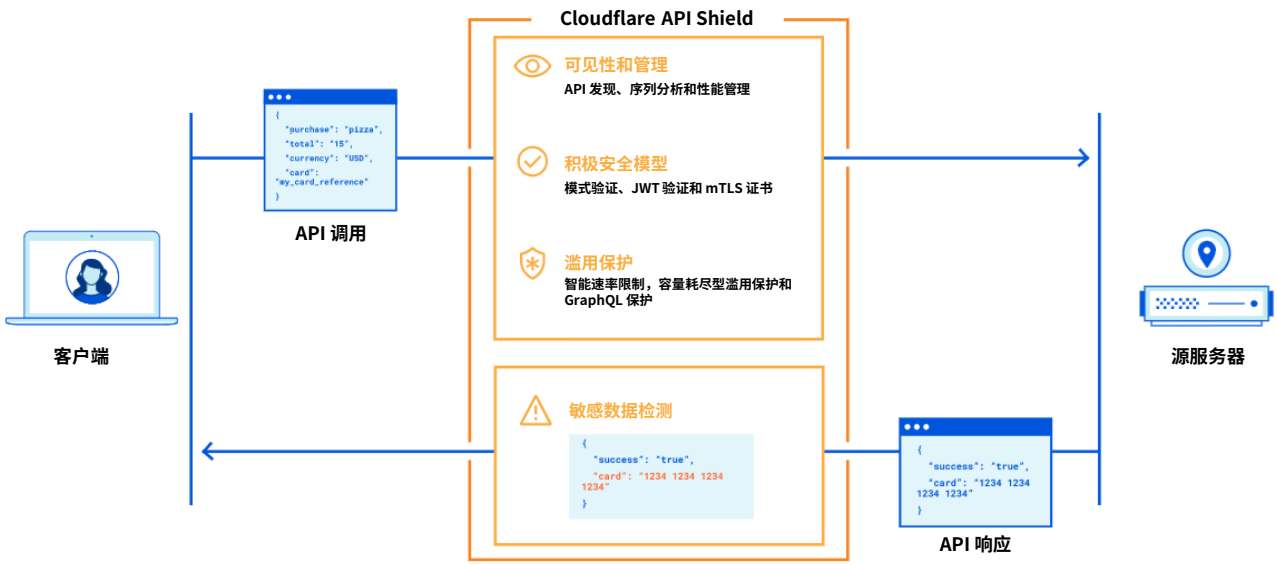

图 1： Cloudflare API Shield 架构

Cloudflare 领导地位

Cloudflare 应用安全产品因其实力和广度而赢得无数荣誉。Cloudflare 在最新的 Forrester Wave：Web 应用防火墙报告中获评为“领导者”。2023 年度 Gartner® Peer Insights™ “客户之声”：DDoS 缓解解决方案报告将 Cloudflare 评为 “客户之选领导者”。Forrester 在 2024 年第三季度 Forrester Wave™：机器人管理软件报告中将 Cloudflare 评为“表现卓越者”。Cloudflare 在 2024 年 IDC MarketScape Web 应用和 API 保护 (WAAP) 企业平台报告中获评为“主要参与者”。