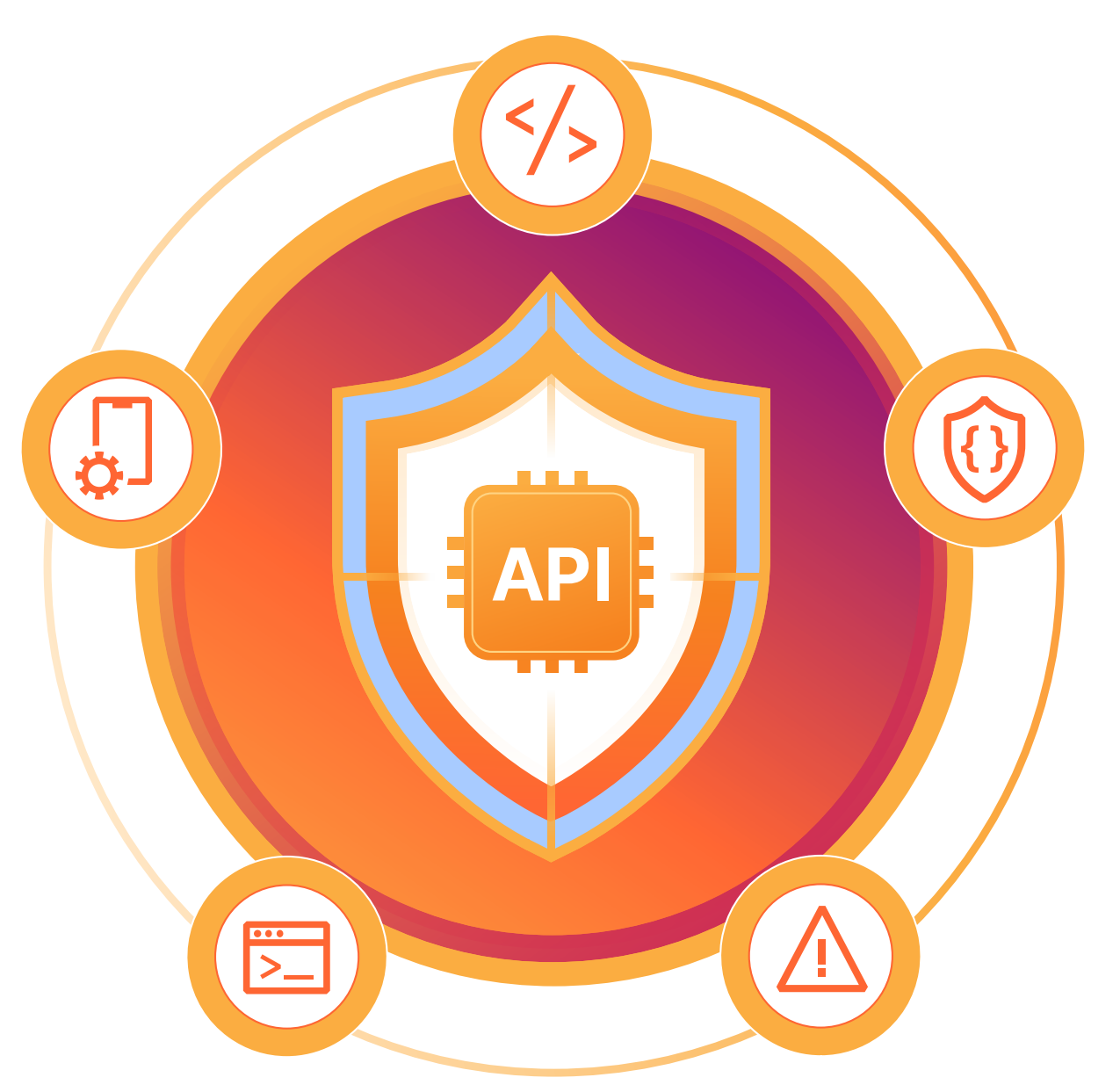
API 安全性與管理現狀



應用程式開發介面 (API) 推動全新的應用程式體驗——從追蹤健康資料到個人化線上遊戲。它們還推動了無數的商業優勢：客戶分析、SaaS 整合、產生型 AI 功能，等等。

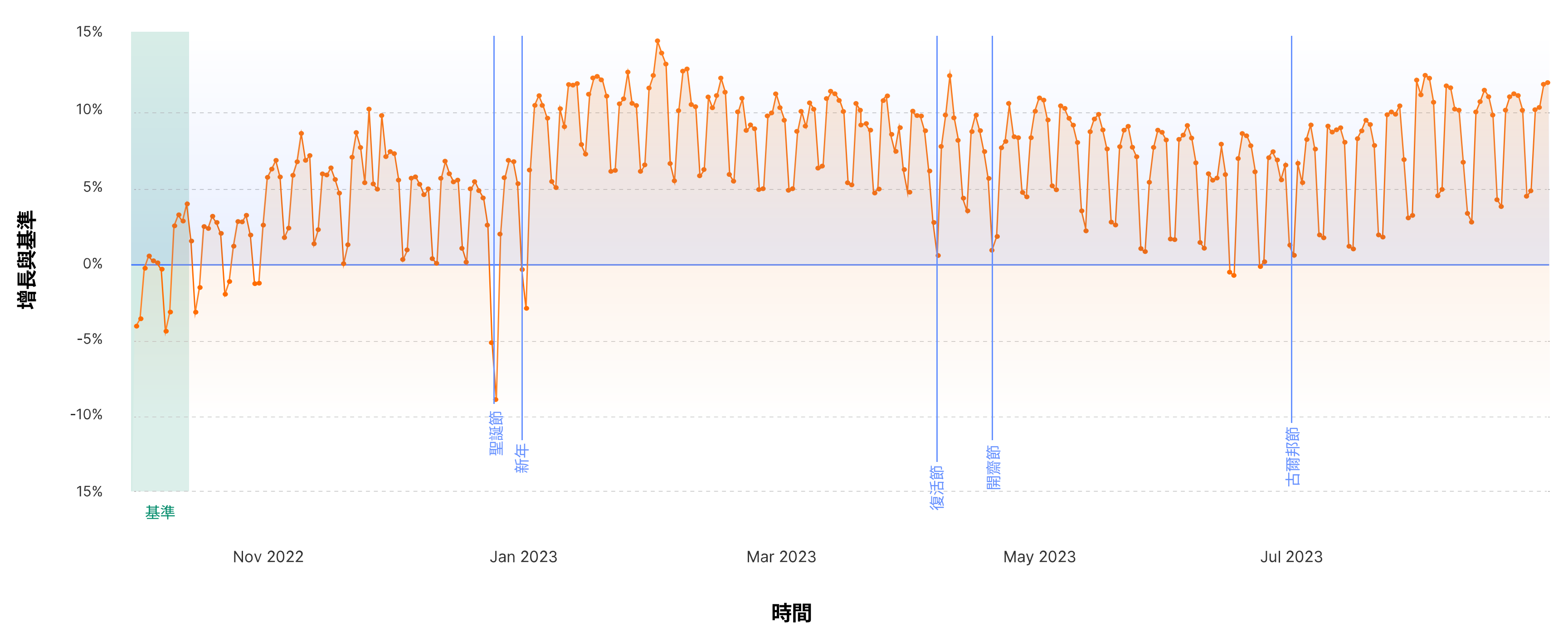
同時，API 管理起來十分複雜，並不斷受到攻擊。看一看 API 流量的安全性和管理趨勢，該流量目前佔**所有動態網際網路流量的一半以上 (57%)***。

30.7%

透過機器學習比透過客戶提供的工作階段識別碼發現的 API REST 端點多了將近 31%

以 API 為中心的世界

總體而言，全球 API 總流量在 2023 年全年穩步增長。



API 流量在整體 Web 流量中所佔份額最高的 10 大產業：

1. IoT 通訊平台
2. 鐵路、公車和計程車
3. 法律服務
4. 多媒體、遊戲與圖形軟體
5. 物流、供應鏈與運輸
6. 消費電子
7. 金融軟體
8. 安全與調查
9. 銀行、金融服務和保險業
10. 醫療裝置

未受保護的 API

缺乏全面 API 詳細目錄的組織面臨「影子 API」的風險——其本質為隱藏的攻擊面：

59.2%

向錯誤的人員提供 API「寫入」存取權可能會導致安全風險。許多 (59.2%) 組織允許對其至少一半的 API 進行「寫入」存取（即推送更新的能力）。

15,000+

超過 15,000 個使用 Cloudflare 的帳戶僅透過機器學習方法探索 API 端點

常見 API 漏洞

隨著 API 流量、錯誤和攻擊的增長，對 API 安全性和管理的市場需求也同時急劇增長。

API 的頭號威脅

HTTP 異常作為最常見的 API 威脅，是惡意 API 要求的常見訊號。

API 流量頭號錯誤

來自 API 來源的超過一半 (51.6%) 流量錯誤包含 **‘429’ 錯誤代碼：「太多要求」**。

頭號緩解方法

三分之一的 API 緩解方法包含封鎖分散式阻斷服務 (DDoS) 攻擊。

保護 API 與 Web 應用程式的挑戰

與

Web 應用程式	API
對終端使用者**可見**	對應用程式使用者**不可見**
由**終端使用者**透過 Web 瀏覽器存取	讓**系統和應用程式**交換資料
透過各種使用者互動從後端（使用 HTML、CSS 和 JavaScript）**視覺化資料**。	透過使用定義的格式（最常見的是 RESTful JSON、gRPC、XML、GraphQL）存取伺服器和應用程式來**傳輸資料**。
通常透過封鎖已知惡意流量的**「被動安全性」**模型獲得保護。	透過僅允許經過驗證的流量的**「主動安全性」**模型，獲得更有效的保護。

保護 API 的 3 種主要方式

移轉到「主動安全性」模型與「被動安全性」

在主動安全性模型中，您只接受「已知良性」API 流量（由 API 結構描述定義）。這比被動安全性更有效，後者僅著重於限制「已知不良」API 流量。

套用機器學習以釋放資源並降低成本

機器學習可以發現所有 API 流量（包括攻擊變體）、區分合法流量暴增與惡意傀儡程式流量，並管理其他耗費資源的 API 管理任務。

統一應用程式開發、可見度、效能與安全性

全球連通雲 實現了網路、雲端、應用程式和使用者之間的任意連線，並在應用程式開發和 API 縱深防禦服務之間提供關鍵的連接橋樑。

想要瞭解更多？

閱讀報告

請存取完整的 Cloudflare《2024 年 API 安全性與管理報告》

---

*本資訊圖中的資料發現基於 Cloudflare 全球網路（包括 Cloudflare 的 Web 應用程式防火牆、DDoS 防護、傀儡程式管理和 API 閘道服務）於 2022 年 10 月 1 日至 2023 年 8 月 31 日期間觀察所得的聚合流量模式。

© 2024 Cloudflare, Inc.