CLOUDFLARE

2024 年 API 安全性與管理報告

目錄

按一下章節可跳到所在頁面

報告摘要

網際網路是電腦之間源源不斷的對話流。這些對話通常使用應用程式開發介面 (API) 進行，後者讓我們得以透過全新的方式與軟體和應用程式互動。例如，使用 OpenAI 的 ChatGPT API，不僅讓 Slack 能夠簡化基於聊天的工作流程，還可讓 Booking.com 提供更加個人化的旅遊規劃體驗。

如今，API 超過了其他網際網路流量，去年佔 Cloudflare[1] 所處理的**動態網際網路流量的一半以上 (57%)**。

然而，正如這份《**2024 年 API 安全性與管理報告**》中所討論的，管理和防止濫用 API 也越來越複雜。

例如，很多組織並不瞭解其 API 的準確資訊。與組織自述的 API 端點相比，Cloudflare 透過基於機器學習的探索發現的 API 端點多了 30.7%。[2]

發現的 API 端點多了

30.7%

遺憾的是，組織無法正確保護他們看不到的東西。

如果實施 API 安全性的那些組織未能準確、即時瞭解其 API 環境，**則可能會無意中封鎖合法流量**。

以 Cloudflare 在 2023 年緩解的**頭號 API 用戶端錯誤類別「太多要求」(429) 錯誤代碼**為例。429 代碼並不一定意味著*來自攻擊者的要求太多*。例如，如果導致錯誤的速率限制最初是因分散式阻斷服務 (DDoS) 攻擊而設定的，則實施過於廣泛的錯誤速率限制仍然可能會封鎖合法使用者。（值得注意的是，**DDoS 防護是 Cloudflare 客戶的頭號 API 緩解方法**）。

本報告的目標是為組織提供一個有價值的基準，來**全面評估其 API 端點管理的健康狀況**。畢竟，API 安全性還必須包含資料才能管理可見度、效能和風險。

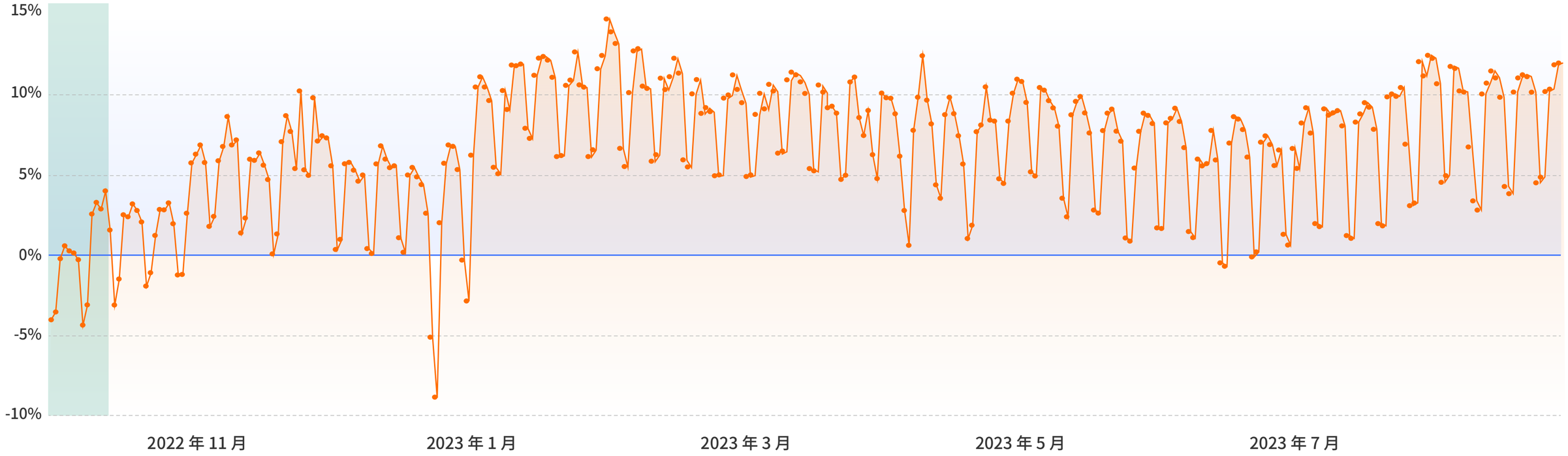
方法

本報告中的調查結果基於 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。Cloudflare 平均每秒處理超過 5,000 萬個 HTTP 要求，平均每天封鎖 1,700 億個網路威脅。

快照：全球範圍內與 API 相關的流量

全球 API 流量隨著時間的推移增長

基準已突出顯示，回應碼為 200，僅限動態快取



2022 年 10 月 1 日至 2023 年 8 月 31 日期間，具有成功回應 (200 狀態代碼) 的 API 流量佔 Cloudflare 動態 HTTP 流量的 53.1% 到 60.1%。動態內容是根據使用者特定的因素 (例如造訪時間、位置和裝置) 而變化的內容。

主要調查結果

API 超過了其他網際網路流量

成功的 API 要求佔 Cloudflare 所處理**網際網路流量**（動態 HTTP 流量）的 **57%**。[1]

頭號緩解方法：DDoS 防護

三分之一 **(33%) 的 API 緩解方法為封鎖分散式阻斷服務 (DDoS)** 攻擊。[4]

未知攻擊面

與組織自述的 API 端點相比，機器學習模型發現的 **API 端點多了將近三分之一 (30.7%)**。[2]

產業變化

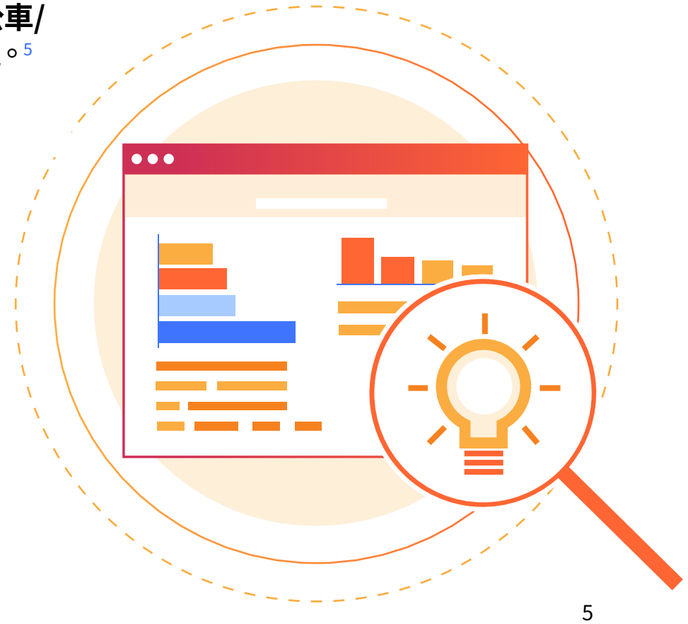
以下產業的 **API 流量佔比最高：IoT 平台、鐵路/公車/計程車、法律服務、多媒體/遊戲以及物流/供應鏈**。[5]

頭號錯誤：太多要求

超過一半 **(51.6%) 的 API 錯誤率為「太多要求」**（429 錯誤）。[3]

地區變化

API 流量佔比在**非洲和亞洲**最高。API 流量**在中東地區變化最大**。[6]



隱藏的攻擊面

對企業而言，API 增強了競爭優勢——更強大的商業智慧、更快速的雲端部署、全新 AI 功能的整合，等等。但是，若要實現 API 最佳化，首先要擁有一份有關主機名稱和暴露於網際網路的所有 API 端點的完整詳細目錄。

如果組織不知曉 API 的存在，則無法對其進行管理或保護。而且，**結果表明，很多組織缺少一份完整的 API 詳細目錄**。

- **Cloudflare 透過機器學習發現的 API REST 端點多了將近 31%**（與透過客戶提供的工作階段識別碼發現的端點相比）。[2]
- ***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。[7]

使用 API 的組織未管理或保護的 API 也稱為「影子 API」，通常由開發人員或個別使用者引入，用於執行特定的業務功能。

儘管它們本身不是惡意的，**但影子 API 本質上是未受保護的攻擊面，會帶來新的風險**。

若被利用，影子 API 可能會導致資料暴露、未修補的漏洞、違反資料合規性、橫向移動以及其他威脅。

可見度檢查

您現在如何探索和編目 API？

一個組織或開發人員的 API 詳細目錄透過 API 結構描述（即定義有效 API 要求和回應規格的中繼資料）擷取。這些 API 結構描述（通常與 OpenAPI 規格一起記錄）包括 API 主機、HTTP 方法、路徑以及開發人員建立的其他要求（例如，路徑和查詢變數）。

目錄

影子 API 的風險

Cloudflare 經常看到組織在 API 管理之旅早期使用「電子郵件和詢問」方法，由此建立的時間點詳細目錄可能會隨著下次代碼發佈而改變。但這種手動方法通常依賴於部落知識，並且容易發生手動錯誤。

假設一個醫療保健組織的 IT 團隊不知道某個 API 允許廠商存取特定系統。如果廠商遭受入侵，則攻擊者可能會濫用該 API 來外洩病患資料。

例如，2019 年 Quest Diagnostics 資料外洩暴露了將近 1,200 萬名病患的資料，當時，一個未經授權的使用者獲得了對向計費廠商傳送資訊的 API 的存取權限。

2022 年，澳大利亞電信提供者 Optus 遭到入侵，據報導，原因是攻擊者透過未經驗證的 API 存取了客戶資料庫。

隨著 API 經濟的增長，API 開發、管理和安全性失去控制和複雜性問題也日益增多。

安全性檢查

您如何監控哪些 API 允許「寫入」存取？

彙整所有帳戶 API 後，Cloudflare 發現，**59.2% 的組織允許對其至少一半的 API 進行「寫入」存取**。[8]

「唯讀」(GET) 存取 API 會從系統中提取和擷取資訊。然而，「寫入」（POST、PUT、DELETE）API 還允許使用者和其他應用程式向系統推送更新（變更）。

許多 API 外洩的發生是因為授權過於寬鬆：使用者被授予太多權限，或者被允許存取其他使用者的資料。當 API 向錯誤的人員提供「寫入」存取權時，就會導致本報告中所述的那些攻擊。

常見 API 錯誤

在組織準確發現（然後儲存或移除）API 端點後，他們需要瞭解哪些進展順利，哪些不順利。API 錯誤可能指示網路攻擊或應用程式效能問題，這會反過來阻止合法業務。

HTTP 狀態代碼是 3 位數代碼，最常用於表明應用程式是否成功執行或是否存在錯誤。

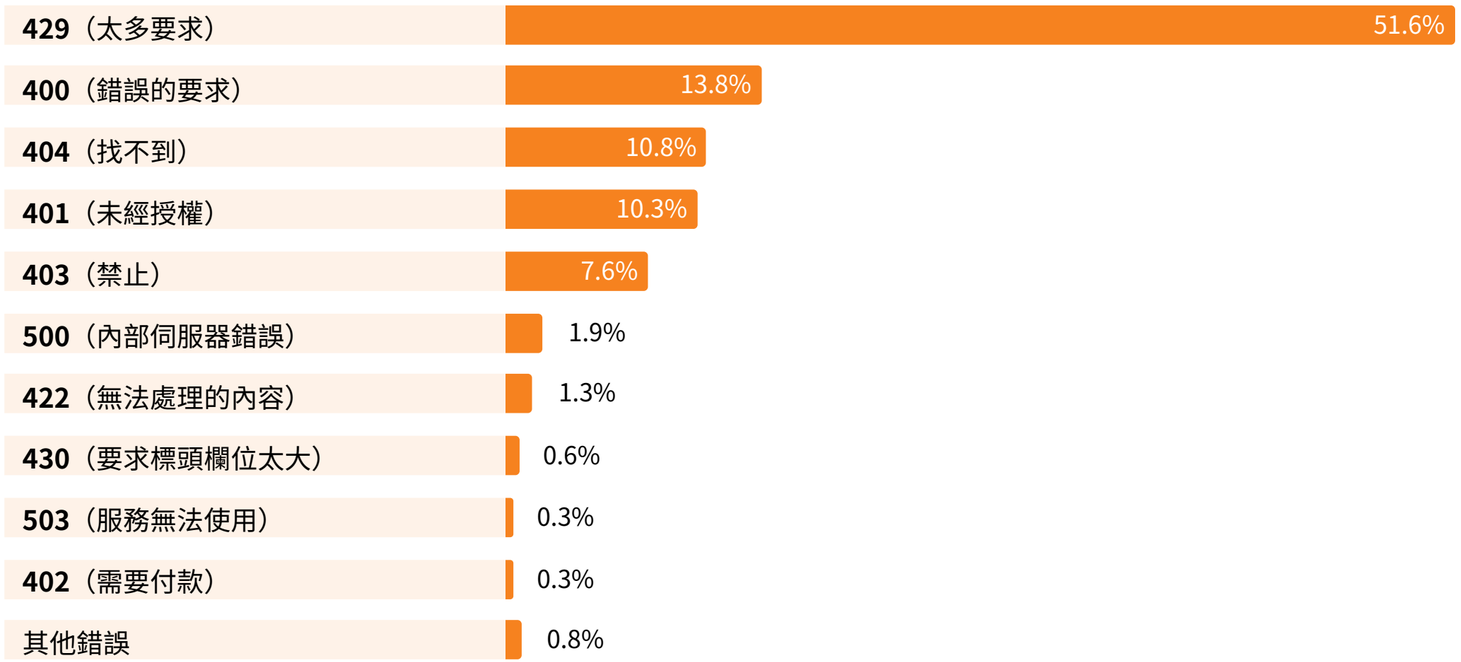
對於 API 和其他 HTTP 要求，以 '2' 開頭的狀態代碼（2xx 成功碼）表示，用戶端的動作已接收、理解和接受（即成功）。

然而，當應用程式訪客無法到達預期目的地時，可能會被重新導向（3xx 重新導向）或遇到 4xx 用戶端錯誤或 5xx 伺服器端錯誤。

Cloudflare 觀察到數萬億的來自 API 來源的流量錯誤，其中**超過一半 (51.6%) 為 '429' 代碼：「太多要求」**。[3]

429 錯誤也稱為「限速」，當用戶端在特定時間內向伺服器傳送了太多要求，就會發生該錯誤。

常見 API 錯誤



請參閱附錄瞭解錯誤描述

誤診 API 錯誤的風險

429 錯誤（最常見的 API 錯誤，如上文所述）表示，當特定動作發生（例如，特定 IP 位址超過每分鐘對 /login 端點的特定要求數）時，伺服器自動限制了 API 流量。

然而，如果組織使用手動設定的限速（而不是自適應限速），則那些要求可能很快就會過時。如果 /login 端點因為成功的行銷活動而非攻擊出現高於平均水平的流量，會怎樣呢？在那種情況下，手動限速可能會阻止合法交易。

另一個錯誤（原因通常為「誤診」）範例是 **401「未經授權」錯誤（Cloudflare 在 API 流量中觀察到的第四常見的錯誤）**。

401 表示使用者的認證不存在或不包含適用於所要求資源的存取權限層級。但就像其他 HTTP 錯誤代碼一樣，該代碼可能是因為一個威脅（例如，一起未遂的無效的物件層級授權攻擊，該攻擊可能會導致完整帳戶盜用），也可能只是因為合法使用者意外輸入了錯誤的認證。

在一個「誤診」API 流量的範例中，2023 年初，Google 警告網站擁有者和一些內容傳遞網路不要使用錯誤的狀態錯誤來限制其（合法的）Googlebot 的編目速率。

正如 Google 提醒使用者的那樣，*「用戶端錯誤只是：用戶端錯誤 … 它們只是表示用戶端的要求在某種程度上是不好的。」*

效能檢查

您如何監控和評估 API 錯誤？

並非所有 API 錯誤都是攻擊造成的。瞭解 API 錯誤的根本原因（以及這些問題背後的趨勢）需要對 API 流量進行一致的記錄，並分析一段時間內的趨勢。

您知道您有多少 API 流量被限速嗎？有多少遭到禁止（因為錯誤授權）？您是否確認錯誤原因是攻擊，而不是使用者認證過期（或輸入不準確）？

主要 API 安全性漏洞

防止濫用 API 極具挑戰性。與其他 Web 應用程式安全服務相比，它們需要更深入的業務環境、探索方法和存取驗證控制。

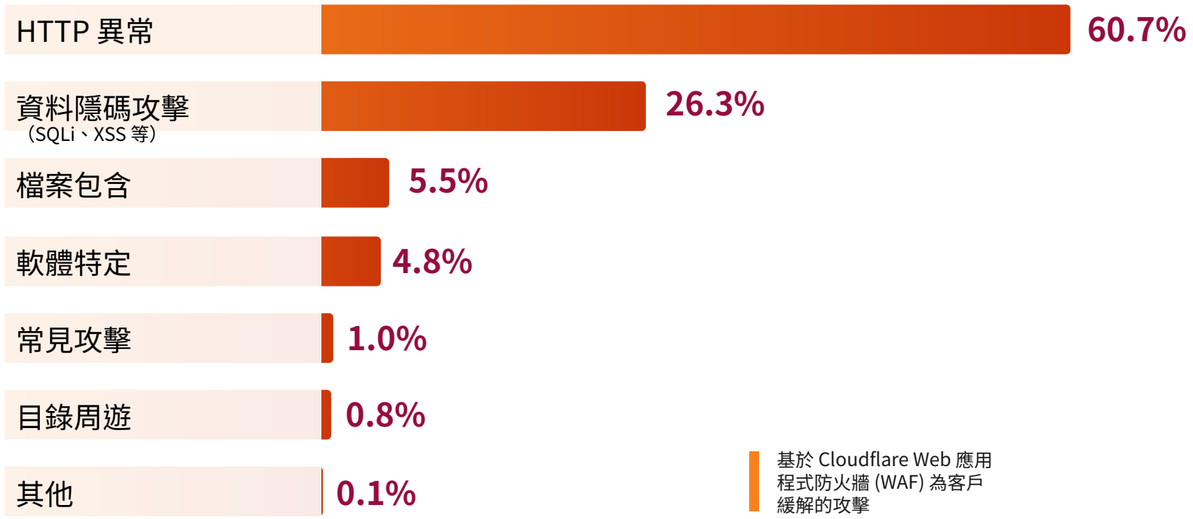
例如，考慮一下：

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**終端使用者存取**（透過 Web 瀏覽器）	讓**系統和應用程式**交換資料
視覺化資料，透過各種使用者互動從後端（使用 HTML、CSS 和 JavaScript）進行。	**傳輸資料**，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。
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之流量的**「主動安全性」**模型，獲得更有效的保護。

出於以上（及其他）原因，定期和自動監控 API 對於即時識別並解決安全威脅至關重要。

以下是 Cloudflare 在 2023 年為客戶緩解的最常見 API 威脅的快照[9]：

主要 API 威脅



如需上述攻擊類型的詳細描述，請參閱附錄。

API 漏洞在一次 MDM 攻擊中的作用

行動裝置管理 (MDM) 可協助組織透過單一平台管理所有地理上分散的裝置。使用 MDM，IT 團隊可以透過裝置內建的 API 在受管理裝置上部署並控制應用程式。

然而，MDM 系統的易用性和便利性必須與風險進行權衡：MDM 系統可以為攻擊者提供對數千台行動裝置的升級存取權限，因此，成為極具吸引力的目標。

2023 年 8 月，美國網路安全和基礎架構安全局 (CISA) 和挪威國家網路安全中心 (NCSC-NO) 發佈了聯合網路安全公告，警告稱攻擊者將兩個漏洞鏈接起來，以**利用 Ivanti Endpoint Manager Mobile (EPMM，原名為 MobileIron Core)**。

攻擊者使用了多種方法，例如，下表中概述的 MITRE ATT&CK® 技術。遵循 MITRE ATT&CK 和 OWASP API 十大安全風險等架構有助於為更具彈性的網路安全 (包括更強大的 API 防禦) 提供堅實的基礎。

技術範例 *(如需完整清單，請按一下這裡)*	**使用**
利用面向公眾的應用程式	至少自 2023 年 4 月以來，攻擊者在面向公眾的 Ivanti EPMM 設備中利用了 CVE-2023-35078。
命令和指令碼解譯器	攻擊者可能利用了 CVE-2023-35081，在 EPMM 裝置上上傳 webshell 並執行命令。
帳戶探索：網域帳戶	攻擊者利用了 CVE-2023-35078 來收集 EPMM 裝置使用者和管理員。 **在這種情況下，他們使用 API 路徑** /mifs/aad/api/v2/authorized/users **列出 EPMM 裝置上的使用者和管理員。**
遠端系統探索	攻擊者擷取了 LDAP 端點。
伺服器軟體元件：Web Shell	攻擊者在遭入侵的基礎架構上植入了 webshell。
代理	攻擊者利用遭入侵的 SOHO 路由器代理至基礎架構並進行入侵。

緩解常見 API 漏洞的兩種方式

1. 結構描述驗證

HTTP 異常（例如，缺少使用者代理程式（為終端使用者擷取網際網路內容的軟體）、格式錯誤的方法名稱、非標準連接埠等）是常見的惡意要求訊號。而且，如上所述，上述類型的 HTTP 異常構成了 Cloudflare 緩解的絕大部分 API 威脅。

結構描述驗證是一種識別 HTTP 異常的重要方式，以便僅允許每個 API 的「乾淨」流量傳送至您的 API 伺服器。API 結構描述基於數個要求屬性（如目標端點、路徑或查詢變數格式以及 HTTP 方法），定義哪些 API 要求是有效的。

2. 解決驗證漏洞

公用 API 中缺乏驗證（或驗證受損）是另一個嚴重的問題，這一點從以往有關 API 相關資料外洩的新聞標題中也可以看出來。

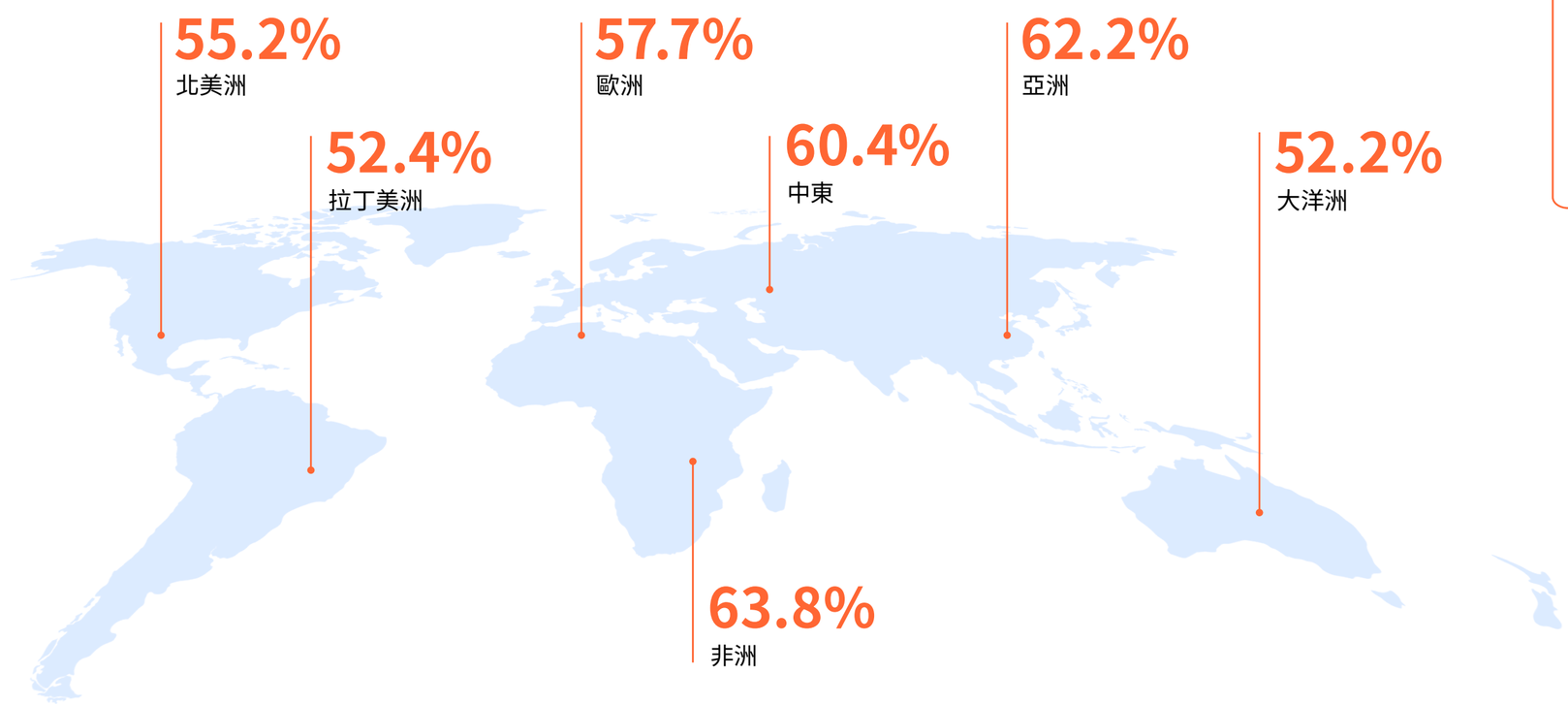
以下四種方式可解決透過 API 暴露敏感性資料的驗證漏洞：

- 首先，除非存在企業核准的例外，否則對每個可公開存取的 API 強制執行驗證
- 限制針對伺服器的 API 要求的速度，以減緩潛在攻擊者的速度
- 封鎖異常的敏感性資料流出量
- 阻止攻擊者跳過合法的 API 要求序列

以 API 為中心的世界

地區趨勢

在 Cloudflare 保護的每個地區中，API 流量佔該地區動態 HTTP 流量的一半以上[10]：



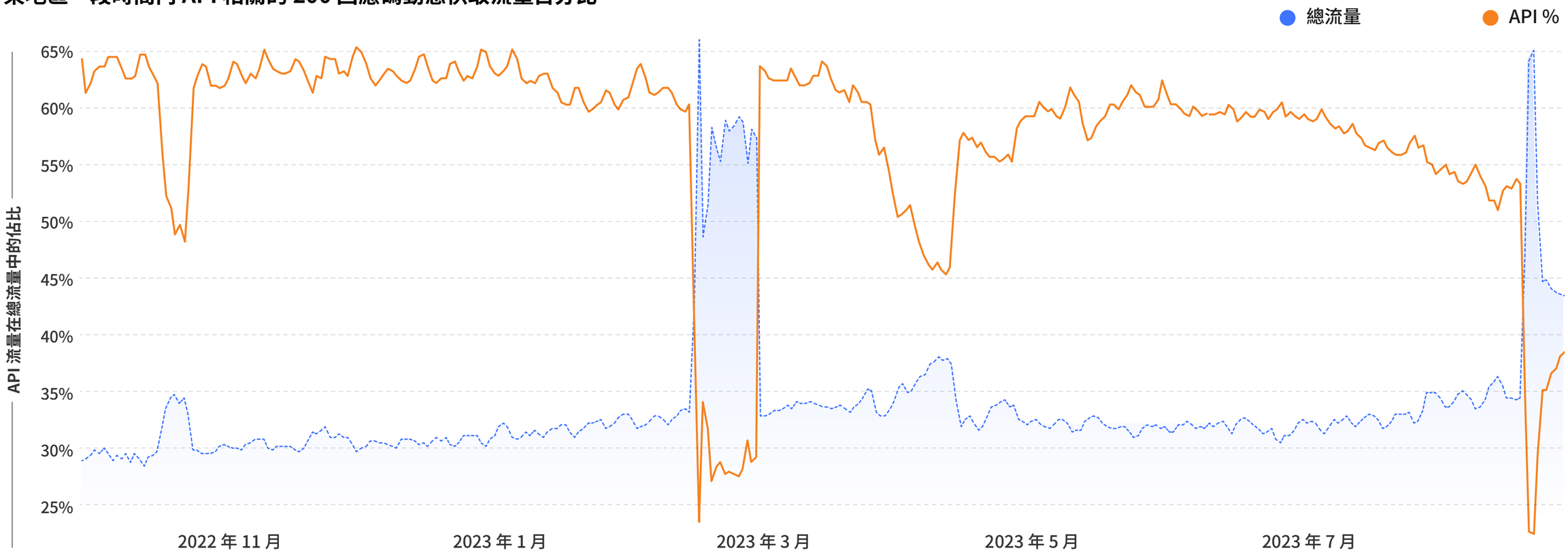
總體而言，API 總流量在 2023 年全年穩步增長。然而，以下地區出現了明顯的波動：

- 在**拉丁美洲**，API 流量佔動態 HTTP 流量的**46.1% 至 58.6%**
- 在**大洋洲**，API 流量佔動態 HTTP 流量的**44.1% 至 57.4%**
- 而在**中東地區，API 流量的變化最大**，下節將對此進行討論。

中東地區流量暴增

在中東地區 API 流量大幅波動的同時，**一款匿名工具的整體流量**（這款工具以協助規避網路限制而聞名）突然出現短期的飆升。Cloudflare 觀察到，2023 年該匿名工具流量暴增出現在政府指示的網際網路關停之後不久。

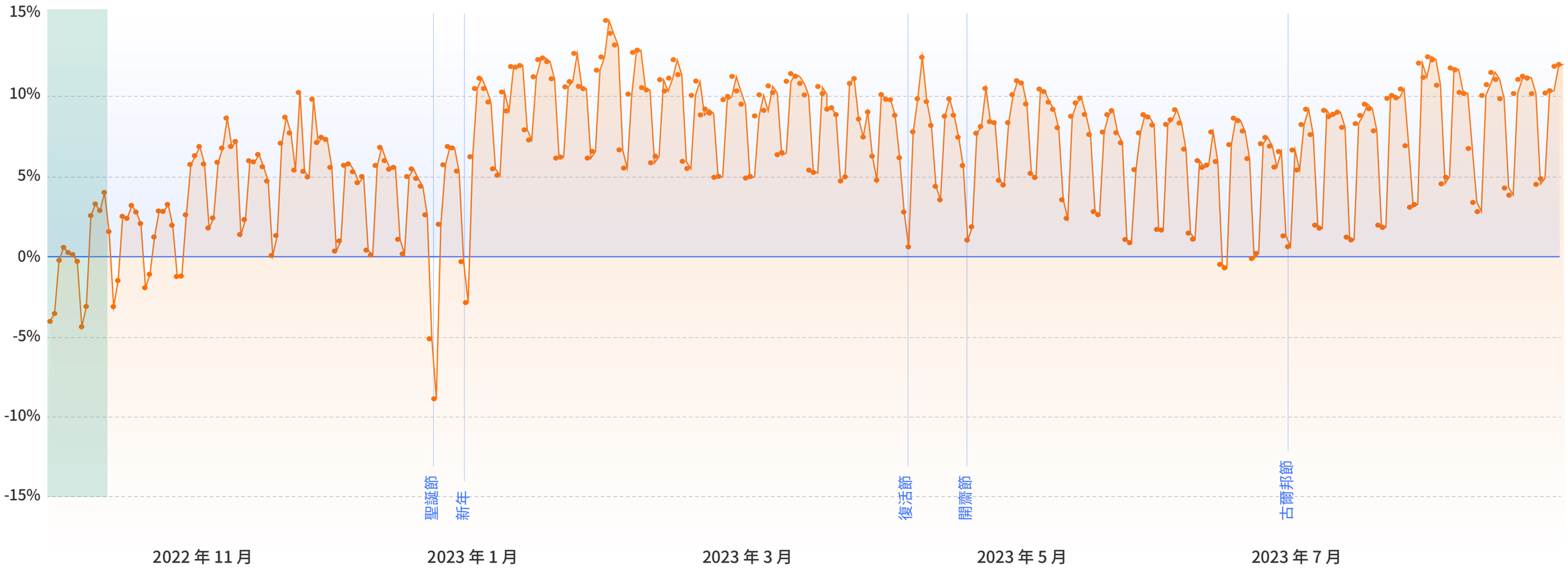
中東地區一段時間內 API 相關的 200 回應碼動態快取流量百分比



API 流量放緩了嗎？

儘管 API 流量通常被認為是傀儡程式之間的交談，但 Cloudflare 的資料卻顯示，API 流量在全年都有明顯的升降，尤其在重大節假日前後。

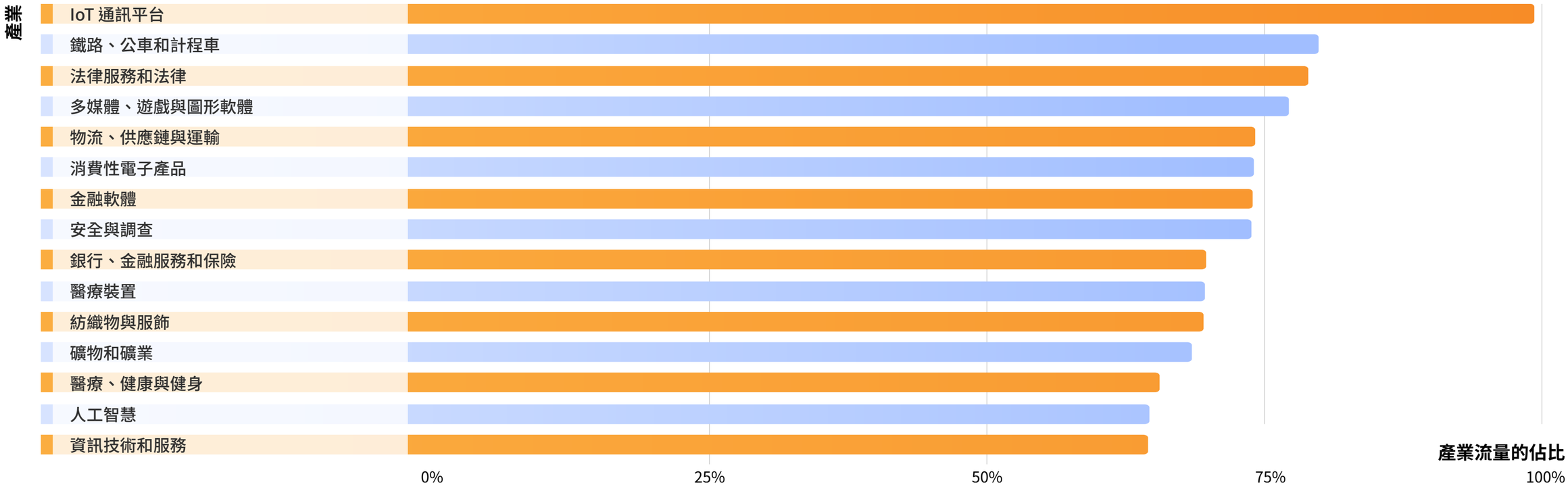
似乎當人們更有可能離線時（例如，**12 月 25 日（聖誕節）、4 月 9 日（復活節）或 4 月 22 日（開齋節），API 流量明顯下降**。[11]



不同產業的 API 流量

除了地理變化以外，**某些產業的 API 流量佔比也大於其他產業**。

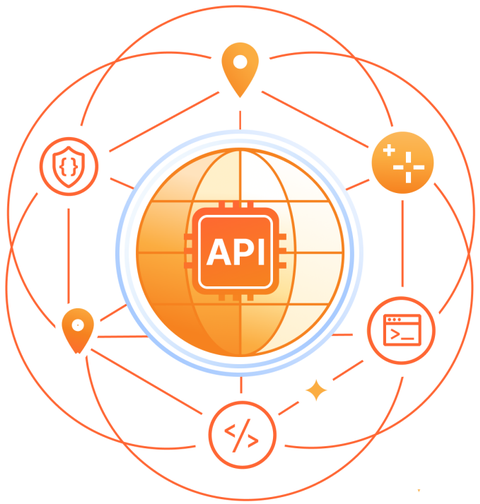
Cloudflare 觀察到 API 驅動的流量較高（與該產業的動態 HTTP 總流量相比）的前 15 個產業[12]
如下所示：



產業基準

任何應用程式、網站或行動應用程式都可以透過 API 新增功能來豐富使用者體驗，而無需從頭開始建立新功能。

例如，共乘應用程式可以透過付款公司的 API 新增付款服務，而不需從頭開始建立自己的付款服務；零售 API 透過虛擬試衣間、產品推薦和訂單狀態協助實現個人化客戶體驗。



API 在任何地方、任何產業都很有用。

以下是特定地區 API 流量佔比最高的產業[12]：

非洲

1. **設施服務**
2. 礦物和礦業
3. 資本市場
4. 募款
5. 信用卡與交易處理

亞洲

1. **IoT 通訊平台**
2. 礦物和礦業
3. 紡織物與服飾
4. 銀行、金融服務和保險業
5. 人工智慧

歐洲

1. **多媒體、遊戲與圖形軟體**
2. 內容與協作軟體
3. 醫療裝置
4. 紡織物與服飾
5. 法律服務

拉丁美洲

1. **礦物和礦業**
2. 金融軟體
3. 多媒體、遊戲與圖形軟體
4. 資本市場
5. 律師事務所

中東

1. **募款**
2. 法律服務
3. 無線
4. 資本市場
5. 運輸/貨車運輸/鐵路

中東

1. **法律服務**
2. 鐵路、公車和計程車
3. 消費電子
4. 安全與調查
5. 物流、供應鏈與運輸

北美洲

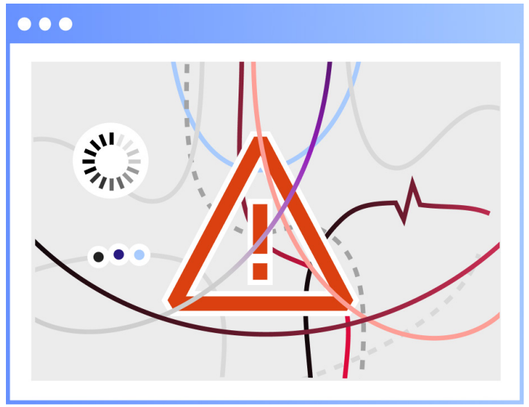
1. **礦物和礦業**
2. 紡織物與服飾
3. 資本市場
4. 安全與調查
5. 製藥、生物技術與健康

對 2024 年及以後的預測

隨著消費者和終端使用者不斷期待更快速、更動態的 Web 和行動體驗，開發和 API 團隊將面臨更大的壓力，需要部署和維護更多的 API。這些善意的應用程式開發人員將繼續快速部署 API——有時並不會諮詢其他 IT 和安全性利害關係人。

這種缺乏凝聚力的方法將迫使企業陷入困境，因為他們面臨著以下挑戰：

1 失去控制和複雜的局面愈演愈烈



IT 決策者表示，導致對 IT 和網路安全環境失去控制的首要因素是「應用程式總數」，其次是「應用程式位置增加」。

然而，在大多數組織中，這些團隊仍然是孤立的：

73% 的開發人員表示，網路安全團隊要求他們做的工作或使用的工具「干擾了他們的工作效率和創新」。

87% 的 CIO 認為，軟體工程師和開發人員「在安全策略和控制方面作出妥協，以更快地將新產品和服務推向市場」。

<50% 的 CISO 認為，開發人員「非常熟悉」開發和工作流程工具的安全風險。

IT、安全性和應用程式開發團隊都有責任保護擁有數千個支援 API 的資產所涉及的龐大攻擊面。

除非企業使用自動化 API 保護修復 IT、安全性和應用程式開發之間的脫節狀態，**否則 API 風險和管理複雜性均會增加**。

2 AI 更易於獲得，導致 API 風險增多

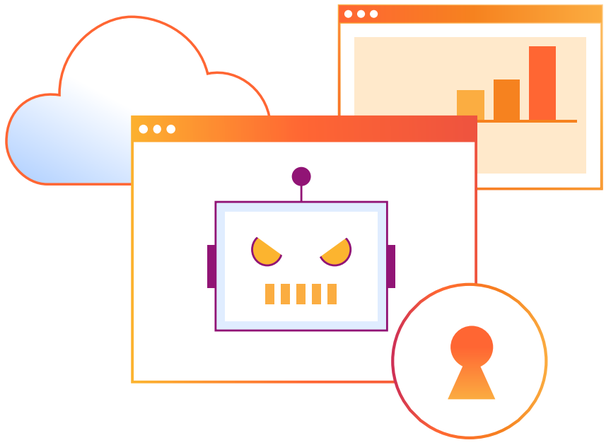
分析師預測，到 2026 年，超過 80% 的企業將使用產生型人工智慧 (GenAI) API 或模型，並且/或者在生產環境中部署支援 GenAI 的應用程式（例如 ChatGPT）。

GenAI 模型（如果沒有 Web 應用程式前端）通常作為內部功能直接存取，或者由其他應用程式和使用者透過公用 API（例如，OpenAI 的 ChatGPT 和 Whisper API）存取。**因為 GenAI 的使用大大增加了 API 的使用，GenAI 服務也會吸引更多 API 相關攻擊來攻擊其 API**。

例如，如果競爭對手或攻擊者「呼叫」一個產品 API 數百萬次來剽竊和竊取資料，則相對於受害者的基礎架構帳單而言，他們的直接成本可以忽略不計。但是，如果攻擊者透過 API 利用目標受害者的產生型模型，則成本要高得多——每次呼叫需要數美分。如果攻擊者對 AI 應用程式的 API 發起數百萬次濫用呼叫，則會立即造成財務損失。

而且，即使出於善意利用 GenAI，對於很多開發人員來說仍然是全新的未知（也意味著高風險）領域。Forrester 預測，2024 年，如果不採取適當的防護機制，「至少有三次資料外洩會被公開歸咎於 AI 產生的不安全程式碼——由於產生的程式碼本身的安全瑕疵，或者 AI 建議的依存性中的漏洞」。

3 基於商務邏輯的欺詐攻擊增加



21 世紀 20 年代，傀儡程式操作者瞄準了 Web 應用程式，它們使用檢測版本的 Web 瀏覽器來建立基於瀏覽器的複雜傀儡程式。同時，大多數現代應用程式在幕後使用 API 來完成使用者動作，例如，帳戶建立、登入、表單填寫和貨幣交易工作流程。

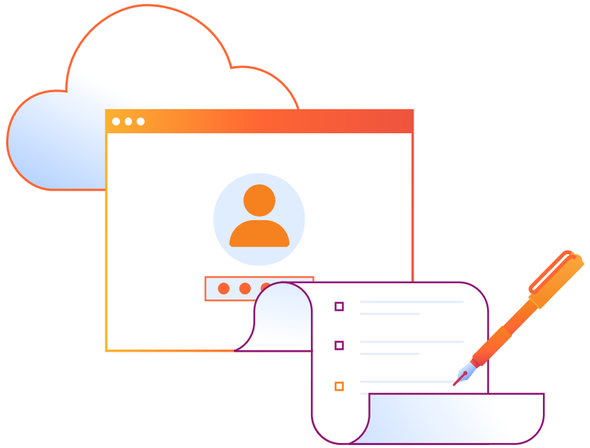
我們預計，2024 年，傀儡程式操作者將越來越多地直接攻擊那些工作流程背後的 API，因為此類攻擊更高效（API 的變更頻率往往低於 Web 應用程式 UI），而且 API 受保護程度較低（與 Web 應用程式相比）。

以在體育博彩和夢幻聯賽中建立虛假帳戶為例。如果一個人針對不同的賭注和球隊陣容擁有多個帳戶，則會增加獲勝概率，這通常可以轉換為金錢獎勵。因此，激勵自動大規模建立新帳戶甚至更加有利可圖。

類似的激勵也出現在憑證填充攻擊（不存在多重要素驗證，或者可以輕鬆繞過）和欺詐性購買限量供應物品中。

在此類情況下，組織需要在 API 安全工具中使用基於商務邏輯的智慧。例如，識別攻擊者嘗試的異常序列以快速追蹤其欺詐企圖。以及識別 API 呼叫何時具有異常行為特性，例如，嘗試以比該 API 的基準交易量更快的速度完成交易。

4 法規和控管不斷增加



預計組織還應**增強控管和努力，來監管 API 相關的安全性和隱私權**。

例如，PCI DSS（「支付卡產業資料安全標準」）是一個架構，用於指導企業完成管理持卡人交易和付款驗證資料之流程。2024 年 3 月 31 日，**全新的 PCI DSS 4.0 版要求（第一個要明確解決 API 安全性的版本）將生效**。

隨著 PCI DSS 4.0 版的發佈，傳輸或處理卡付款的任何組織都必須解決 API 漏洞、確保適當的 API 驗證，等等。如果未遵守 PCI DSS 要求，則可能會導致巨額罰款和其他懲罰。

醫療保健是另一個受嚴格監管的產業，鑒於 API 能夠在系統之間傳輸受電子保護的健康資訊 (ePHI)，預計會對其進行更多的審查。

2023 年 7 月，美國聯邦貿易委員會以及衛生和公眾服務部的民權辦公室 (OCR) 對健康應用程式的隱私權風險加強了審查，其發出警告，將對未披露個人健康資料外洩情況的行為進行經濟懲罰。

建議

就像任何軟體一樣，API 漏洞也會發生。雖然無人能夠阻止攻擊者不斷地嘗試新策略來破壞應用程式和 API，但組織可以使用包含以下最佳做法的全方位方法來識別、保護和管理 API：

1 使用全球連通雲，統一管理應用程式開發、可見度、效能與安全性

很多企業擁有專屬的基礎架構、獨特的合規性需求，以及非完全相容的程序和設定，因此很難將 SaaS 應用程式、Web 應用程式和其他 IT 基礎架構連接起來。這些網域在構建之時並未考慮到輕鬆、安全地協同工作。

全球連通雲是一種全新的方法，用於為公司提供保護和連接數位環境所需的多種服務。它是一個可程式設計的雲端原生服務的智慧平台，支援網路、雲端環境、應用程式和使用者之間的任意連線。

全球連通雲在應用程式部署和 API 縱深防禦服務之間提供了連接橋梁，這些服務包括：

- **自動化 API 探索和可見度**，為組織提供清晰的 API 資產詳細目錄
- **現代驗證和授權**流程在初始時已內建
- **API 端點管理**，用於監控 API 驅動的網域的指標，例如，延遲、錯誤和錯誤率，以及回應大小
- **API** 第 7 層 (L7) **保護**，包括進階限速和 DDoS 防護，來應對阻斷服務攻擊、暴力登入嘗試以及其他 API 濫用
- **偵測 zero-day**（在沒有修補程式或修正程式的軟體中發現的新漏洞），以防發生 zero-day 攻擊

2 使用 API 閘道移轉到「主動安全性」模型

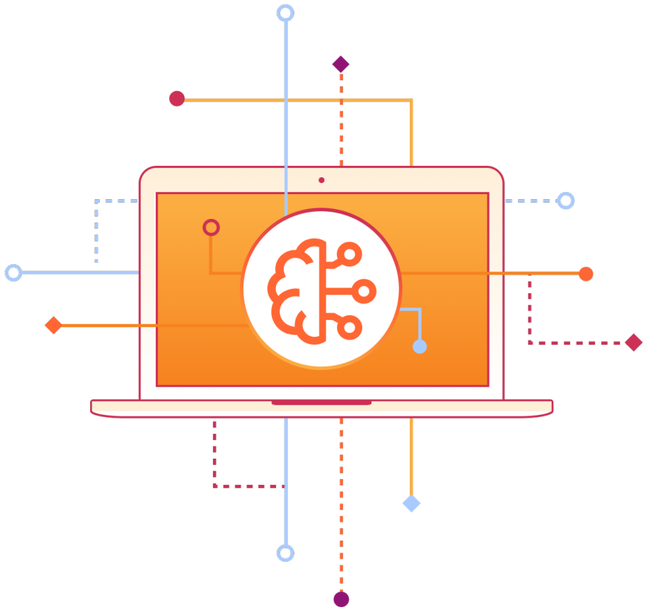
據估計，正在使用的公用和私人 API 有 2 億個（並在不斷增加），IT 和網路安全領導者實際上無法「跟上」每個 API 的效能、行為和風險暴露。

以往，Web 應用程式使用由 Web 應用程式防火牆 (WAF) 強制執行的「被動安全性」模型進行保護，該模型允許除了來自問題 IP、ASN、國家/地區、具有問題簽章（例如，SQLi 嘗試）之要求以外的所有內容。這是因為使用者可以透過多種方式存取 Web 應用程式並與之互動。在這樣的模型中，WAF 將封鎖「已知不良」流量，並允許所有其他流量。

相比之下，API 的「主動安全性」模型更適合，因為 API 有一個結構化格式來與之進行互動。與被動安全性方法相反，**主動安全性模型僅允許「已知良性」行為和身分（「良性」由 API 結構描述定義）**，而拒絕其他一切內容。

使用主動安全性模型的組織透過僅接受符合其結構描述的流量來保護其 API。他們可以更有效地封鎖格式錯誤的要求和 HTTP 異常，例如，憑證填充攻擊和自動化掃描工具。

3 使用機器學習技術，釋放資源並降低成本



如果沒有自動化和專門構建的 API 工具，IT 和網路安全利害關係人就不可能跟上 API 團隊。

然而，組織可以透過使用基於機器學習的安全服務，來提高 API 可見度和安全管理效率。例如，透過機器學習，可以快速：

- **發現**某個網域的所有 API 流量（包括未經驗證的 API），而不考慮基於工作階段識別碼的資料
- **偵測** API 上的 RCE、XSS 和 SQLi 攻擊變體
- **訓練**一個分類器來區分各種流量類型和 API 攻擊手段
- **區分**應用程式使用者流量的合法峰值和潛在惡意傀儡程式流量的峰值

4 隨著時間的推移，衡量並改進您組織的 API 成熟度

最全面的保護 API 的方法是實作一個全方位的 Web 應用程式和 API 保護 (WAAP) 平台。但是，一個剛剛開始承認其 API 暴露風險的組織可能無法在一夜之間發現此方法的可行性。

然而，所有進展都需要從某個地方開始。在組織瞭解需要保護的內容之後，就可以不斷努力，從而實現全面的 API 管理和安全性：

第 1 級：可見度

公司必須先追蹤並正式管理所有 API 端點，包括任何影子 API。然而，很多組織都無法像開發人員構建 API 那樣快速地找到自己的 API。而且，當他們找到 API 後，也很難為潛在的數百個 API 端點中的每一個準確構建唯一的結構描述。

透過 API 可見度服務，組織既可以自動探索 API 端點，也可以識別誰擁有該 API 以及應如何使用該 API。

第 2 級：一般 Web 攻擊防護

Web 應用程式和 API 通常協同工作（例如，一個使用 API 處理付款的電子商務網站）。然而，網際網路的全球特性將網站和其他應用程式暴露於來自多個位置、具有各種規模和複雜度層級的攻擊。

以下是「基本」服務的範例（如需詳細資料，請參閱這裡），用於直接保護 Web 應用程式及其背後的 API 免受 DoS 和 DDoS 攻擊、憑證填充、zero-day 漏洞以及其他威脅類型：

- **DDoS 緩解服務**位於伺服器和公共網際網路之間，用於防止惡意流量激增而導致伺服器不堪重負
- **Web 應用程式防火牆 (WAF)** 可篩選掉已知（或疑似）利用 Web 應用程式漏洞的流量
- **加密憑證管理**可協助管理 SSL/TLS 加密過程的關鍵元素
- **進階限速**可保護端點免遭 DoS 攻擊、暴力登入嘗試以及其他 API 流量激增，而不會影響合法使用者。

第 3 級：API 特定攻擊防護

WAF 和 DDoS 等工具對 Web 安全性和（人類）應用程式使用者的體驗至關重要，但這些服務旨在保護應用程式，而不是專門保護 API。

隨著組織透過 API 公開更多的服務，他們應使用專門構建的 API 安全性和管理來增強 Web 應用程式安全性。

使用無監督機器學習的進階 API 安全性能夠針對每一個 API 開發單獨的基準，並在發出 API 要求時預測其意圖（合法還是惡意）。

組織明白，團隊中的很多人對 API 安全性都很陌生。實現安全性並不是為了安全性本身，而是為了改進和提高業務成果。其好處包括：加快產品交付速度、減少已發佈 API 的安全漏洞、提高網路安全團隊效率，並最終提高開發人員和 API 團隊的工作效率。

在 API 推動業務發展的同時為其提供安全保護

在 Cloudflare 全球連通雲的支援下，Cloudflare 的 Web 應用程式和 API 保護 (WAAP) 產品組合整合了頂級應用程式安全功能，來確保應用程式和 API 安全高效、阻止 DDoS 攻擊、封鎖傀儡程式等。

進一步瞭解

Cloudflare 的 API 探索、OWASP API 十大安全風險防護、mutual TLS 以及保護 API 且無損創新。

目錄

API 安全性字彙

API 呼叫或 API 要求：一條傳送至伺服器並要求 API 提供服務或資訊的訊息。

API 探索：API 探索是對組織內使用的所有內部和第三方 API 進行編目的過程。

API 端點：履行 API 要求（也稱為 API 呼叫）的地方。API 端點幾乎始終在伺服器上託管。

API 流量：任何含有 XML、JSON、gRPC 或類似回應內容類型的 HTTP 要求。如果回應內容類型無法用於緩解的要求，則會改為使用同等的 Accept 內容類型（由使用者代理指定）。在後一種情況下，不會完全將 API 流量列入考量，但是為了深入解析之用，還是具有相當不錯的代表性。

傀儡程式流量/自動化流量：任何由 Cloudflare 的傀儡程式管理系統識別為由傀儡程式產生的 HTTP 要求。

無效的物件層級授權 (BOLA)：BOLA 是對要求內的物件 ID 進行操作，以獲取對敏感性資料的未經授權的存取。使用 BOLA，攻擊者只需變更 ID 即可存取本不應該能夠存取的物件（資料）。

失效的使用者驗證：如果驗證實作不正確，攻擊者可能能夠冒充 API 使用者，從而存取機密資料。

用戶端：發出 HTTP 要求的一方。通常是在瀏覽器上存取網站的終端使用者，但也可能是 API 用戶端或從網站要求資源的任何人。

目錄周遊：目錄周遊也稱為路徑周遊攻擊，旨在存取儲存於 Web 根資料夾外部的檔案與目錄。

分散式阻斷服務 (DDoS) 攻擊：DDoS 攻擊是指透過使用大量網際網路流量使目標或其周圍的基礎架構不堪重負，惡意嘗試中斷目標伺服器、服務或網路的正常流量。

檔案包含：此漏洞可讓攻擊者在目標應用程式中包含檔案。在未經適當驗證的情況下使用使用者提供的輸入會導致該漏洞。

HTTP 異常：HTTP 異常（例如，格式錯誤的方法名稱、標頭中有空值位元組字元、非標準連接埠，或是含有 POST 要求且長度為零的內容）是 Cloudflare 受管 WAF 規則所緩解攻擊的常見指標。如需 HTTP 異常規則範例的詳細描述，請參閱這裡的 Cloudflare 部落格。

資料隱碼攻擊類型範例包括：

- **命令資料隱碼**：攻擊者透過易受攻擊的應用程式在主機作業系統上執行任意命令的情況。
- **Cross-site scripting (XSS)**：XSS 是一個漏洞，允許攻擊者將用戶端指令碼插入 Web 應用程式中，以便直接存取重要資訊、假冒成使用者或藉由欺騙使用者來竊取重要資訊。
- **SQL 資料隱碼攻擊 (SQLi)**：這種方法能讓攻擊者以資料庫執行搜尋查詢的方式鑽漏洞。攻擊者使用 SQLi 取得未授權資訊的存取權限、修改或建立新的使用者權限，或是操縱或毀損機密資料。

HTTP 要求：網際網路通訊平台（例如 Web 瀏覽器和應用程式）透過這種方式索取其載入資源所需的資訊。

已緩解的流量：曾經由 Cloudflare 平台套用過「終止」動作的任何瀏覽型 HTTP* 要求。其中包括 BLOCK、CHALLENGE（例如 CAPTCHA 或 JavaScript 型查問）等動作。此流量不包括套用過以下動作的要求：LOG、SKIP、ALLOW。

限速：在電腦系統中用於控制要求處理速率的一種技術。它可以用作一種安全措施來阻止 API 攻擊，或限制來源伺服器中的資源使用。

遠端程式碼執行 (RCE)：攻擊者在組織的電腦或網路上執行惡意程式碼。執行攻擊者控制程式碼的能力可用於多種用途，包括部署其他惡意程式碼或竊取敏感性資料。

結構描述驗證：如果 API 要求不符合 API 的結構描述，API 可能會以意想不到的方式做出反應，比如洩露機密資料。結構描述驗證使 API 能夠丟棄此類要求。

Zero-day 漏洞：這些是應用程式製造者不知道的漏洞，因此沒有可用的修復程式。攻擊者希望盡快利用這些漏洞。

HTTP 狀態代碼描述

以下狀態代碼範例（這些是最常見的 API 錯誤，如第 8 節中所述）詳細描述了 Cloudflare 如何解釋 HTTP 回應碼的網際網路標準追蹤通訊協定。如需瞭解本通訊協定的標準化狀態，請參閱目前的《網際網路官方通訊協定標準》版本 (STD 1)。

429 表示**太多要求**。用戶端在指定時間內向伺服器傳送了太多要求。通常稱為「限速」。伺服器可以回應一段資訊，讓要求者在一段特定的時間後重試。

400 表示**錯誤的要求**。用戶端未向伺服器傳送正確的要求。這是一個用戶端錯誤：格式錯誤的要求語法、無效要求、建立訊息框架或詐騙性要求路由。

404 表示**找不到**。來源伺服器找不到或不願找到所要求的資源。這通常意味著主機伺服器無法辨識 API URL，而這可能是由多種不同的原因造成的。

401 表示**未經授權**。使用者的認證不存在或不包含適用於所要求資源的存取權限層級。

403 表示**禁止**。如果要求違反了為所有橙色雲端 Cloudflare 網域而啟用的預設 WAF 受管規則或為該特定區域而啟用的 WAF 受管規則，Cloudflare 將提供 403 回應。如果您看到一個沒有 Cloudflare 品牌的 403 錯誤，則它始終是從原始 Web 伺服器直接傳回而不是從 Cloudflare 傳回的，並且通常與您伺服器上的權限規則相關。

500 表示**內部伺服器錯誤**。一條通用錯誤訊息，用於指示伺服器端的意外錯誤。

422 表示**無法處理的內容**。要求中存在語意錯誤。

503 表示**服務無法使用**。伺服器可能因維護或原始 Web 伺服器過載而關閉。

430 表示**要求標頭欄位太大**。此錯誤代碼不是官方代碼，但 Shopify 用它來表示要求未被接受，因為該要求可能是惡意的，並且 Shopify 已經拒絕了它，以保護應用程式免遭任何可能的攻擊。

402 表示**需要付款**。並未廣泛使用，但一些平台在超出每日限額或付款出現問題時使用該代碼。

章節附註

1. Cloudflare 全球網路平均每秒處理 5,000 萬個 HTTP 要求，峰值高達每秒 7,000 多萬個 HTTP 要求。2022 年 10 月 1 日至 2023 年 8 月 31 日期間，具有成功回應 (200 狀態代碼) 的 API 流量佔 Cloudflare 動態 HTTP 流量的 53.1% 到 60.1%。動態內容是根據使用者特定的因素 (例如造訪時間、位置和裝置) 而變化的內容。
2. 對於 REST API 端點，與在所有客戶網域/區域透過客戶提供的工作階段識別碼發現的端點相比，Cloudflare 的 API 探索透過機器學習發現的端點平均多了 30.7% (260 個與 199 個)。
3. 基於 2022 年 10 月 1 日至 2023 年 8 月 31 日期間最常見的非 2xx HTTP 狀態代碼 (包括 4xx 和 5xx 錯誤) 佔 API 所有 HTTP 錯誤 (動態快取狀態) 的百分比。
4. 為了計算緩解的 API 流量，Cloudflare 計算了每個 Cloudflare 產品來源緩解的 API 流量的每日百分比，以及受管規則依據 Web 應用程式防火牆 (WAF) 規則類別緩解的流量的每日百分比。
5. API 流量佔該產業動態 HTTP 總流量 70% 以上的主要產業 (依據組織的 Salesforce 產業類別)。
6. 基於北美洲、歐洲、拉丁美洲、大洋洲、亞洲、非洲和中東地區傳回成功 (200) 回應碼的 API 流量在 Cloudflare 網路處理的所有動態 HTTP 流量中的佔比。
7. Cloudflare 有兩種方法進行 API 探索：查看包含工作階段識別碼的流量，以及使用基於 ML 的探索引擎 (無需工作階段識別碼)。有 15,431 個帳戶僅透過 ML 探索端點。
8. 基於每個帳戶的 API 總數，細分為具有寫入存取權 (PUT、POST、PATCH、DELETE) 的端點和具有「僅資訊」(GET) 存取權的端點。為了撰寫本報告，Cloudflare 計算了 GET API 至少佔每個客戶 API 總數 50% 的帳戶百分比。
9. 基於依據 Cloudflare WAF 受管規則類別為客戶緩解的 API 流量
10. 基於每日 API 百分比中位數，根據用戶端所在國家/地區內傳回 200 回應碼和動態快取的 API 要求數量 (在具有動態快取的所有 200 回應碼流量中的佔比) 計算得出。
11. 基於 API 流量與全球基準 (平均) 每日 API 流量相比的每日百分比變化。
12. 基於該產業的動態 HTTP 總流量與其他產業的比較情況，其中「產業」由客戶帳戶的 Salesforce 產業類別定義。

致電：+ 886 8 0185 7030
電子郵件：enterprise@cloudflare.com
造訪：www.cloudflare.com/zh-tw/

REV:BDES-5122.2024JAN04