白皮書 | 2016 年 12 月

為企業使用者選擇正確的 API 管理解決方案

API 機會

應用程式設計介面 (API) 可能已經變成舊觀念，不過這個觀念正在經歷轉型，因為有更多組織受到行動裝置和雲端需求的影響而對外部開發人員開放本身的資訊。藉由透過 API 將資料提供給開發人員使用，這些公司 (如 eBay、Expedia 和 Salesforce) 已在新市場中取得銷售佳績。根據 ProgrammableWeb.com 的數據，透過網際網路提供的開放 API 數現在超過 16,000 個，在 2005 年只有 32 個。[1]

對外部開發人員開放 API 使得許多技術創業公司得以成為平台，讓開發人員社群結合核心資料或應用程式資源。這造就了新的接觸面 (例如 Twitter 的快速成長)、營收 (例如 Salesforce.com 的 AppExchange) 或一般使用者保留 (例如 Facebook)。

使用 API 對外部開發人員分享資訊和功能並不限於技術創業公司。越來越多企業在雲端、行動裝置和合作夥伴三方面整合方案的推動下，使用 API 讓企業成為開發人員生態系統的中心，藉以透過本身的資訊資產擴大新的接觸面、營收和保留的可能性。然而，與許多創業公司不同的是，企業必須非常謹慎處理 API 發佈，因為他們要承受的風險相當多，包含名譽、規範以及對於客戶、合作夥伴、員工和股東的共同需求。

企業 API 管理挑戰

將 API 發佈到合作夥伴設立的或對外開放的外部開發人員社群，都會使企業面臨許多挑戰和風險。您如何保護資訊資產免於不當使用或攻擊？您如何提供可靠的 API 服務，而不造成會影響停 API 使用者的停機？您如何透過以原則為依據的一致方式控管 API 的存取和使用？您如何透過 API 獲利？您如何協助開發人員瞭解 API 並自行管理本身的存取？雖然這些問題都與創業公司和企業兩者有關，不過對於企業 IT 組織而言更加尖銳急迫。原因不僅是企業無法承受倉促的 API 管理策略可能會帶來的名譽損害，也是因為企業需要維持審慎的 IT 流程和安全防護。

不過，無論企業想要使用何種 API，都需要能夠因應一些基本功能區域的 API 管理解決方案：

- **API 安全性** — 企業無法承受濫用或不當使用由 API 提供的資訊或任何應用程式資源。
- **API 生命週期管理** — 企業需要設法確保 API 更新不會在升級/修訂 API 或在環境、地理區域、資料中心和雲端之間移動時中斷。
- **API 控管** — 透過如計量、SLA、可用性和效能等原則特性，企業需要一種方法來控制和追蹤 API 如何公開給不同合作夥伴和開發人員的更廣泛運作特性。
- **部署彈性** — API 管理解決方案應該與企業現有的基礎架構整合。
- **開發人員啟用及社群建置** — 企業需要設法讓開發人員進行作業、管理這些開發人員，並協助開發人員充分使用所提供的 API。
- **API 獲利** — 對於部份企業而言，發佈 API 還不夠。API 同時也代表新的營收機會，而不同的 API 管理解決方案可達成不同程度的獲利。

對於企業而言，因應這些功能需求毫無妥協餘地。不過，對於這些功能需求，企業預期 API 管理解決方案展現對於本身獨特的 IT 使用相關聯的運作特性。

- **解決方案安全性** — 由於 API 管理解決方案是在「非軍事區 (DMZ)」中部署，因此企業也需要穩健的 IT 等級 API 解決方案能夠滿足各種安全性需求，從深入防護到 PCI 合規性、FIPS 和 API 金鑰安全性的 HSM 支援。
- **解決方案管理能力** — 企業具有跨地理區域、資料中心和雲端的開發、測試和生產環境，這表示 API 管理解決方案必須符合其特定的開發模式和程序。
- **解決方案可靠性** — 企業發佈 API 在商業上期待極高的運作時間，並且無法承擔中斷的狀況。

穩健且可行的解決方案有何特性？

本白皮書檢視這些不同的功能和運作需求，為 IT 管理員、網路管理員和企業架構師提供選擇 API 管理解決方案的重要資訊。

API 管理解決方案功能需求

API 安全性

尋求 API 管理解決方案時，安全性功能通常是首選要件，尤其在買方是尋求透過與 SOAP、REST 或 JSON 之類的標準無關的 API 防護重要資訊的企業時。API 安全性顧慮首先出現在存取控制。對於對外的 API，這表示需要能夠：

- 接受不同類型的認證用於驗證
- 將不同類型的認證發給開發人員
- 支援不同的資源授權機制，包括 OAuth、OpenID Connect 和 SAML 之類的同盟機制

對於企業而言，這項挑戰由於與現有身分基礎結構整合的需求而更顯複雜。因此，整體目標是達到彈性和整合。原則上，應該能夠支援不同類型的存取權杖，甚至換用不同類型的開發人員 API 金鑰，而完全不需要改動程式碼。解決方案應該能夠支援各種 OAuth 機制，假設這些就是行動安全性和 API 的標準，而且能夠處理各種 OAuth 樣式，例如金鑰雜湊訊息鑑別碼 (HMAC) 以及與企業標準 (例如安全聲明標記語言，SAML) 的組合。當然，API 管理解決方案也需要搭配 CA、IBM、Oracle 和 RSA 等公司的既有身分投資。

不過，API 安全性並不僅止於存取控制。API 為您的資料開啟了一道程式設計的視窗，這就是為什麼企業等級 API 管理解決方案需要讓企業架構師或安全性管理員細部控制公開哪些資料、這些資料如何保密，以及如何確保資料傳輸不遭受攔截或竄改。

此外，API 安全性取決於 API 本身和其所使用資料/功能的完整性，而這需要可確保 API 不會受到攻擊、拒絕服務或濫用而遭到破壞的能力。良好的 API 管理解決方案能夠為操作員提供許多威脅防護控制，確保 API 及其通訊的可用性和精確度。

API 生命週期管理

API 並非一蹴可幾。和任何應用程式功能一樣，API 也需要從設計到撰寫程式碼、測試和部署的開發生命週期。無論開發程序採行瀑布模型或敏捷開發方式，都需要能夠在開發生命週期追蹤 API 的變更。這就是為什麼 API 管理解決方案需要具有全功能的工作流程以用於：

- 使用業界標準計畫和設計 API
- 從點到點整合和保全 API
- 測試、部署及因應修訂和復原
- 管理和監控 API 使用情況，包含報告和分析

全功能 API 管理解決方案也應該能夠因應同時生產多個版本，以因應舊客戶或不同的存取技術，如簡易物件存取通訊協定 (SOAP)、具象狀態傳輸 (REST) 和 JavaScript® 物件通知 (JSON)。只能因應本地化開發的生命週期管理架構將無法滿足大多數現今企業的需求。公有和私有雲端的重要性日益成長。這表示企業需要 API 管理解決方案能夠在雲端中跨越測試和生產，也要能夠將 API 開發人員從網路特質和拓撲的變化莫測中隔離開來。

API 控管

控管是一個廣義的詞彙，通常用來描述各種管理、程序和可見度需求，並且定義一或多個取用者使用 API 的條款與條件。雖然控管涵蓋安全性和生命週期概念，不過也顯現不同的 SLA、監控和報告需求。此外，對於 API 管理解決方案而言，控管更需要根據取用者的身分、能力、訂閱層級或其他可以在原則中界定的交易環境，針對不同的取用者在共用 API 資料與功能方面啟用不同的條款與條件。

有效的 API 控管完全在於彈性。控制如何共用 API 的技術只能遵循企業的偏好和程序進行。這表示應該可以使用原則針對任何 SLA、安全性、記錄或其他控制設定 API 管理解決方案。原則是彈性的核心，並確保對於不同的實作保持一致。允許管理員進行各種控制而未界定完整原則 IDE 的 API 管理解決方案，將限制可規範的項目及可進行控制的方式。

部署彈性

多數企業具有設計來輔佐其進行業務的現有基礎架構。當開始使用 API 管理解決方案時，企業應評估增加至其現有環境的解決方案。架構團隊應該要能夠將此解決方案當作其基礎架構的延伸來管理，而非視為個別的環境。如需此整合階段的詳細資訊，請參閱解決方案簡介，《將您的 ESB/SOA 環境延伸至行動裝置、雲端和 IoT 的架構師指南。(An Architect’ s Guide for Extending Your ESB/SOA Environment to Mobile, Cloud, and IoT.)》

開發人員啟用及社群建置

控管 API 可確保發佈者一致的控制，但如果外部開發人員無法輕易找出並使用 API，發佈者就面臨開發人員不使用 API 的風險。因此，現今大多數 API 管理解決方案在控制功能之外提供安全性、生命週期和控管功能，協助發佈者向外部開發人員公開 API 的資訊，這通常透過開發人員入口網站進行。開發人員入口網站提供單一的互動點讓開發人員註冊帳戶、要求 API 存取金鑰、找出可用的 API 和查看範例程式碼。

企業用途的 API 開發人員入口網站應該：

- 提供容易使用的行動 API (包含 OAuth 和 OpenID Connect)
- 為操作員提供報告和分析

- 輕鬆啟用業務關係管理

因為不同的企業使用 API 發佈的經驗和優先順序都不同，所以一體適用的 API 入口網站作法遠不如一體適用的 API 安全性、生命週期和控管架構。這就是為什麼許多企業想要考慮可分解的 API 入口網站。這可以是可自訂以適用特定開發人員投入策略的白標入口網站，或是可由既有企業開發人員入口網站用作個別元件的 API 入口網站。而且，彈性是重點。

API 創造營收

創造營收的概念與開發人員提供的想法有關。雖然許多企業透過允許免費存取網路和行動 API 的方式提高採用率，不過其他企業通常對於較高的存取層級推出付費使用選項。同樣地，解決獲利問題並沒有單一的有效方式。部份選項包括：

- 使用量低於資料傳輸或用戶端要求閾值則可免費使用的免費增值模型
- 對於特定服務保證層級或高於免費使用者的優先順序進行收費
- 提供非付費客戶無法使用的頂級資訊或功能

無論採取何種方法，API 管理解決方案都應該相當縝密，足以讓企業彈性訂定營收基準。解決方案應該能夠：

- 擷取多種使用量統計資料，以建立測量取用的基礎
- 提供進階 SLA 和服務類型功能，以達到流量優先順序設定
- 撰寫可對於付費客戶隔離的虛擬付費型 API，而完全不需要編寫程式碼

API 管理解決方案運作需求

解決方案安全性

由於 API 管理解決方案是唯一能夠使企業 API 對外隔絕的技術，不過授予安全性解決方案層級的 API 必須與解決方案的安全性一樣安全。如果解決方案遭破壞，API 的任何安全性也將遭破壞。因此，檢視 API 管理解決方案的企業應該將解決方案的安全性視為絕對重要的考量。

這些解決方案將做為外界與內部 API 的中介，也就是最先評估的品質標準是解決方案本身是否會遭破壞。這取決於已進行何種深入測試解決方案，對於解決方案的存取進行限制的程度，以及是否符合金鑰漏洞評估。應該考量經過安全性技術實施指南 (STIG) 測試的解決方案、對於將傳送信用卡資訊的解決方案所發給的支付卡產業資料安全標準 (PCI DSS) 憑證、聯邦資訊處理標準 (FIPS) 合規性，

以及需要達到更高政府安全性標準的解決方案適用的通用條件憑證。

基於最切合實際的目的，企業通常採用 Proxy 型 API 管理解決方案處理外界對於內部 API 提出的要求。中介型 API 閘道可明確用於控制和隔離，使安全性憑證和管理更簡化 (就像是使用網路防火牆)。某些產品也提供立即可用的硬體安全模組 (HSM) 支援來將 API 金鑰加密。在許多情況下，API 金鑰主要用來驗證對於不當使用進行的防護，因此透過加密防範這些金鑰遭竊是相當審慎的策略。

解決方案管理能力

不同於典型創業公司從單一 Amazon 實例或小型託管提供者執行整個生產網站，企業一般有不同的開發和生產環境，例如：

- 分散在各地的開發人員團隊
- 跨越全球資料中心的生產環境
- 雲端型災難復原系統

因此，管理能力是任何選擇決定的關鍵因素。如何管理 API 閘道叢集、如何使不同地點達到負載平衡、如何在停止運作的資料中心環境中運作，以及如何處理尖峰負載之類的考量比其他功能更重要。同樣地，並非所有 API 管理解決方案都能夠滿足企業的特定需求，因此您應該先審慎評估各種解決方案如何支援叢集管理、備援、負載突增、災難復原及其他運作管理因素，再著手特定的途徑。

解決方案可靠性

企業決定採用 API 發佈計劃之後，將實際成為 API 取用者的服務提供者，而 API 取用者將依賴企業並期待持續的正常運作。在此情況下，企業將無可避免地在選擇 API 管理解決方案時強調可靠性。企業將尋求內建備援功能並大幅降低或免除停機風險的解決方案。尋求 API 管理解決方案的企業可能會考量下列性質的解決方案：

- 能夠在內部、雲端或透過混合解決方案 (API 閘道內部部署、雲端開發人員入口網站) 部署
- 提供完整備援，不論部署模型為何
- 與您現有的基礎架構整合
- 符合安全要求

結論

因為每個企業都具有不同的需求或環境，所以絕對沒有全部通用的 API 管理解決方案。不過，所有企業都需要絕佳的功能和運作。對於致力於從外部啟動發佈 API 的大多數組織而言，這等同於希望停性的原則導向 API 管理解決方案能夠符合撥叫等級服務提供者的嚴格生產標準。在功能上，它需要 API 管理解決方案能夠符合各種安全性先決條件、因應常見開發生命週期、可透過原則控管、讓開發人員開始作業、讓開發人員投入，並支援獲利的選項。在運作上，API 管理解決方案應該很安全、可管理且可靠。

使用獨立搜尋幫助您選擇 API 管理解決方案

數個頂尖的分析公司涵蓋 API 管理技術並發佈比較廠商的報告，協助企業選擇對其數位策略最佳的解決方案。IT 評論網站 (如 IT Central Station) 也可以成為廠商比較和客戶評論的絕佳資訊來源。

若要取得頂尖分析廠商比較的免費報告，並查看客戶對於 CA API 管理的看法，請造訪：**ca.com/us/products/api-management/why-ca-api-management.html**.

連絡 CA Technologies

我們歡迎您提出任何問題、評論和一般意見反應。

如需詳細資訊，請造訪 **ca.com/api**

如需與 CA Technologies 聯繫，請前往 ca.com/tw

CA Technologies (NASDAQ: CA) 創造的軟體能為公司轉型注入源源不絕的能量，使他們得以掌握應用經濟的良機。軟體是從事各產業之公司的核心。從計畫到開發、管理及安全性，CA 與來自全球的公司通力合作，跨越行動、私有與公有雲端、分散式與大型機環境等限制，一同改變我們生活、交易及溝通的方式。詳情請造訪 **ca.com/tw**。

1 ProgrammableWeb API Directory，2016 年 12 月，www.programmableweb.com/apis/directory

CS200-241661_1216