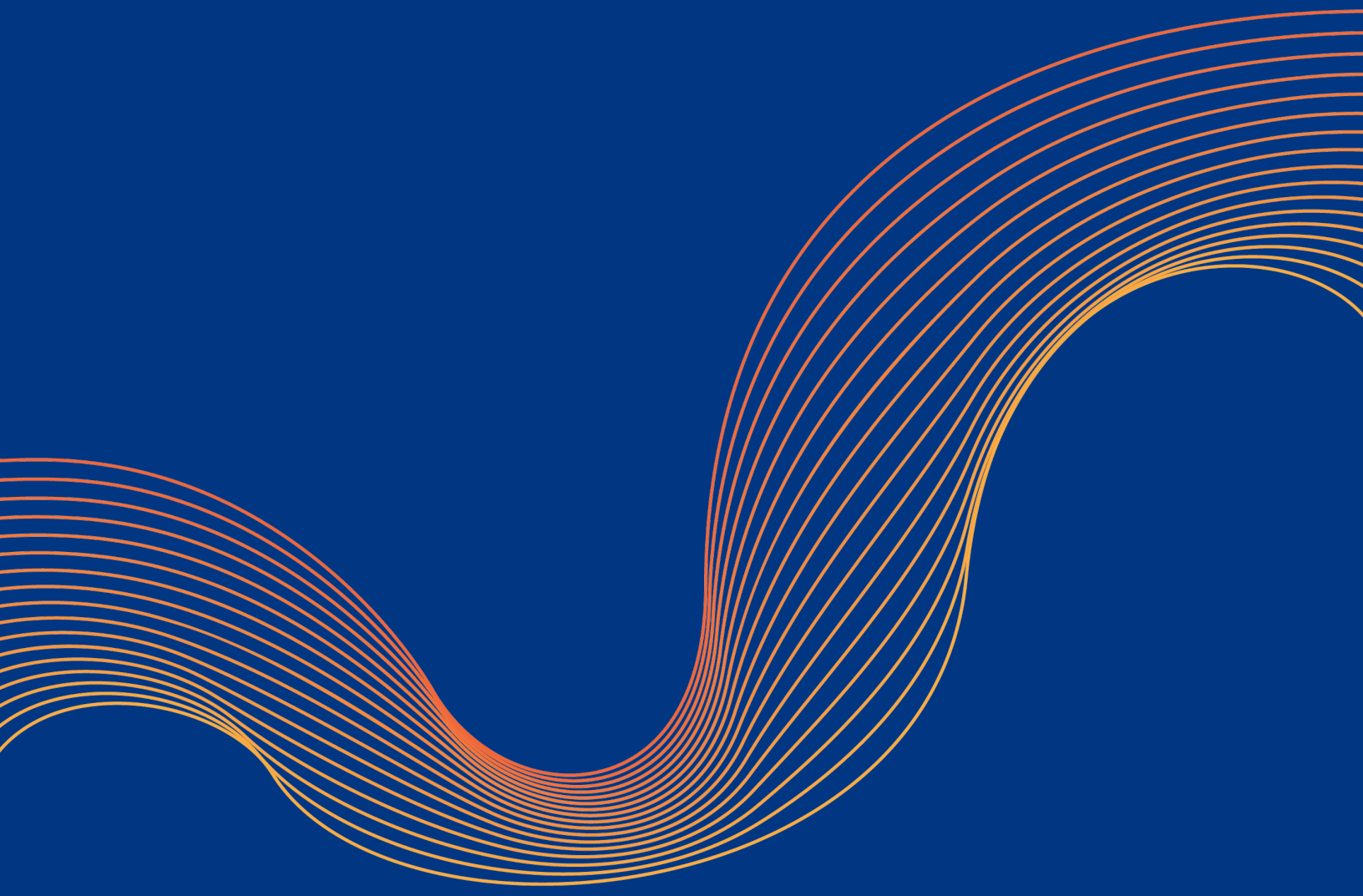
CLOUDFLARE

有效的應用安全需要整體、快速和持續的保護



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

索引

介紹

應用程式安全性威脅一直都存在。在 2020 年，國家漏洞資料庫 (National Vulnerability Database, NVD) 報告有超過 18,000 個漏洞——這創下新的記錄。令人憂心的是，其中有超過 10,000 個漏洞標籤為重大或高度嚴重。

同時，攻擊者持續利用眾所周知的漏洞。來自美國網路安全和基礎結構安全機構 (Cybersecurity and Infrastructure Security Agency, CISA)、聯邦調查局 (Federal Bureau of Investigation, FBI)、英國國家網路安全中心 (National Cyber Security Center, NCSC) 和澳洲網路安全中心 (Australian Cyber Security Centre, ACSC) 的聯合研究發現，2020 年 (以及 2021 年年初) 被攻擊者利用的前 30 個漏洞當中，很多都是眾所周知的漏洞，而且全部都有修補程式可用。

這些知名漏洞的安全風險一直存在，因為公司即使努力修補其軟體亦難以解決漏洞。更糟的是，即使公司嘗試在遭到利用之前修補漏洞，修補過程仍然需要平均 16 天的時間，造成應用程式開放讓人攻擊。

不幸的是，原生漏洞並非應用程式擁有者唯一的安全顧慮。API 會引進本身的風險，而來自 Cloudflare 網路的資料顯示，超過 50% 的請求與 API 相關。此外，機器人占了網際網路流量的 40%，因此機器人攻擊保護變得非常重要。最後，許多網站依賴第三方程式碼，也會讓應用程式開放，遭受供應鏈攻擊。

保護應用程式以抵禦每個一可能的攻擊的不同產品和解決方案，會讓應用程式安全很快就變得分散而且複雜。實施綜合性的應用程式安全策略則有所助益。有效的應用程式安全策略應全面、快速且持續地抵禦一定風險。

應用程式安全顧慮概述

對於應用程式擁有者而言，最迫切的安全顧慮包括：

應用程式漏洞

應用程式內的漏洞極為常見。Veracode 最近的軟體安全報告發現，83% 的應用程式至少有一個安全性缺陷，其中許多應用程式的安全性缺陷超過一個。此外，在研究中，超過 20% 的應用程式至少有一個嚴重缺陷。

API 攻擊

應用程式越來越依賴應用程式開發介面 (API) 來運作。最近，Gartner 預測：「截至 2022 年，API 濫用的攻擊手段將會從不頻繁變成最頻繁的攻擊手段，造成企業網絡應用程式資料外洩。」[1]

[1] Gartner 預測：「截至 2022 年，API 濫用的攻擊手段將會從不頻繁變成最頻繁的攻擊手段，造成企業網絡應用程式資料外洩。」來源：Gartner「API 安全性：保護 API 所需要的事項」，Mark O'Neill, Dioniso Zumerle, Jeremy D'Hoinne，2021 年 3 月 1 日，(需要 Gartner 訂閱)

機器人攻擊

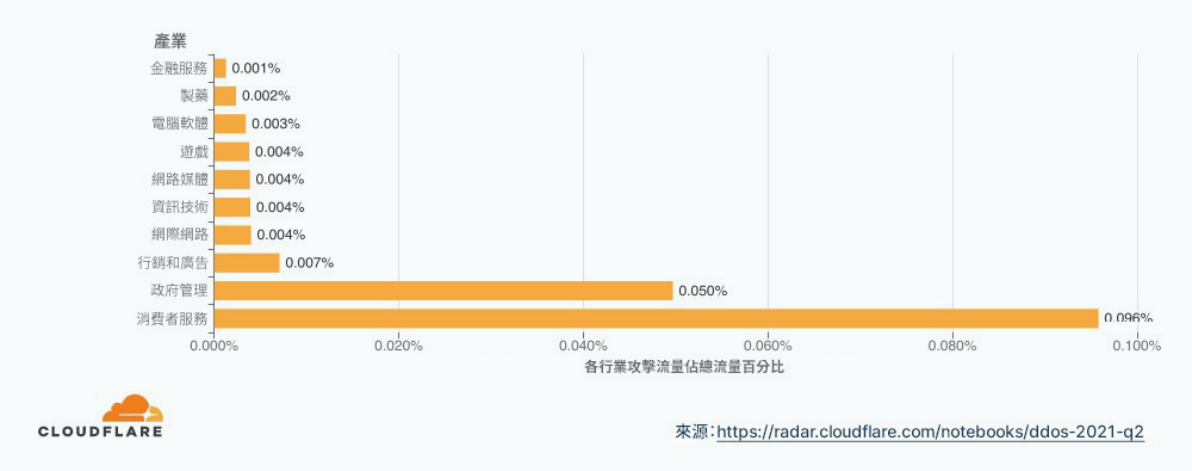
機器人攻擊十分常見。攻擊者通常使用受感染裝置的網路 (稱為機器人網路) 執行各種惡意行為。一個例子是憑證填充，亦即機器人會嘗試將上百或上千個竊取的登入憑證「填充」到登入頁面，希望取得帳戶的存取權限。機器人也會被用來執行內容剽竊攻擊，亦即下載並複製網站內容，以竊取某些搜尋引擎最佳化 (SEO) 利益。

供應鏈攻擊

在供應鏈攻擊中，攻擊者會透過外部來源尋找進入點，例如來自受信任廠商、第三方網站相依性或供應商的軟體。在 2015 年，稱為Magecart 的團體進行了一系列這樣的攻擊——透過惡意程式碼感染網站中依賴的第三方部分，藉此從電子商務網站竊取付款資訊。最終使用者的瀏覽器會載入包含受感染依賴部分的頁面，允許攻擊者從網頁竊取資訊並銷售。這裡指的是透過第三方 (可能是廠商或甚至是網站依賴部分) 運作，會大幅增加攻擊面。

DDoS 攻擊

在 DDoS 攻擊中，攻擊者使用垃圾流量的流入，嘗試攻擊應用程式至離線。不幸的是，DDoS 攻擊者不斷變換規模、使用的手段等。此外，攻擊者也不會慢下來。來自 Cloudflare 網路的資料發現，在 2021 年第 2 季，每 200 個前往美國組織的 HTTP 請求中，就有一個屬於 DDoS 攻擊。



路徑攻擊

應用程式也能成為路徑攻擊的獵物，亦即攻擊者會為了惡意目的，攔截雙方 (例如瀏覽器和伺服器) 之間的通訊。攻擊者可以假冒其中一方並變更通訊或收集敏感資訊。路徑攻擊可以採用多種形式，例如以網域名稱系統 (DNS) 伺服器和電子郵件伺服器等對象為目標。在 DNS 路徑攻擊中，攻擊者會攔截 DNS 查閱流程，並向使用者傳送不同 (通常是犯罪性質) 的網站。同樣地，在電子郵件劫持中，攻擊者會攔截電子郵件伺服器和網絡之間的連線，以便能夠讀取並干擾電子郵件通訊。

抵禦網絡應用程式威脅的最佳做法

防禦這些攻擊類型，應屬於每個組織應用程式安全策略的一部分。但是組織如何防禦這些攻擊也很重要。純熟的應用程式安全策略應為：

- **雲端邊緣網路：**抵禦網絡應用程式威脅的內部部署保護曾經是標準做法，但此方法很難擴充規模。例如，若透過硬體式 WAF 保護應用程式，擴充保護規模的唯一方式是購買額外的硬體。透過更多硬體式保護來佈建應用程式，需要很長的時間，讓應用程式容易遭到攻擊。雲端式解決方案則不會有這樣的問題。這永遠都能提供更大的容量，因此可以無限擴充保護規模。

  除了容量限制，內部部署的保護在購買和維護上的費用也很昂貴。硬體的老化速度相對較快，因此維護或更換成本也會累積。此外，雇用經過訓練的員工來管理硬體，也會增加整體持有成本。相反地，使用雲端式解決方案可大幅降低持有成本。

  雲端式解決方案的另一個優點是可以輕鬆且頻繁地自動更新。這對於網絡應用程式防火牆 (WAF) 等解決方案特別實用，其規則、緩解機制和基礎軟體可在雲端環境下快速更新。相反地，雖然內部部署提供者可以遠端更新解決方案，但流程較為複雜，發生的頻率通常較低。

  雲端邊緣網路進一步採取這些優點。雲端邊緣網路是一組散佈各地、執行相同服務的伺服器。從邊緣提供保護，可讓組織運用雲端的可擴充性優點，同時採用其他相較於集中式模型的效能優勢。

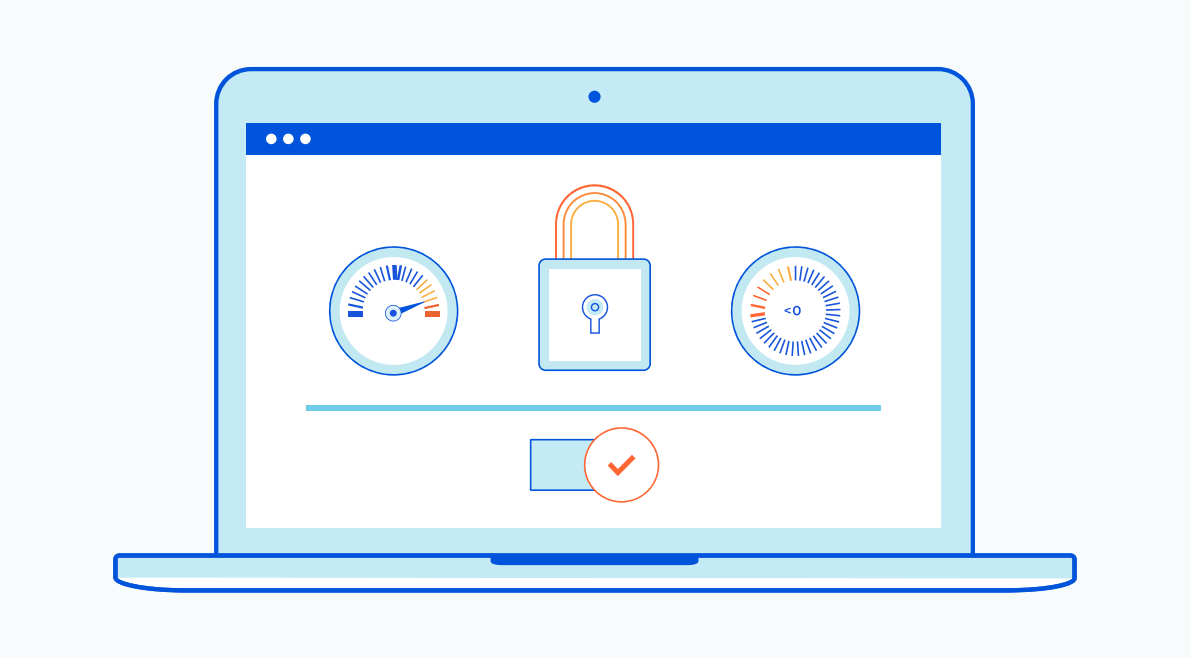
  在雲端邊緣網路中，進行保護的位置會盡可能靠近最終使用者。相反地，在集中式模型中，進行保護的位置是在合併資料中心，與散佈在全球各地的最終使用者距離更遠。為了提供安全性，無論最終使用者位於何處，都必須將所有使用者流量回傳到部署安全性設備的集中式資料中心。例如，若資料中心位於加州，流量將必須先前往該處，再回傳到紐約的最終使用者。

- **統一：**嘗試在多種工具套用一致的保護容易發生錯誤。因此，最好使用單一、統一的系統來防禦攻擊，而非串起多種工具。

  若團隊使用不連貫的工具，通常會讓不同的人管理不同的安全性產品。這可能表示，不會廣泛分享重要資訊，因而產生安全方面的孤立單位和資訊落差。此外，所有工具都需要自己的設定和管理，這會對團隊造成負擔，並導致不必要的複雜性。

  此外，容納太多工具會導致難以剖析所有警示。每個工具都各自有一組傳送警示的規則和邏輯，如果擁有數種工具，會難以判定哪些警示真正重要。

  另一方面，使用統一的系統可讓團隊與較少的工具和集中化的警示互動，因此更容易理解需要注意哪些內容。整合式工具通常也會參考一致的政策，因此更容易套用全域政策。例如，應用程式擁有者可以僅設定一次資料損失預防 (DLP) 規則，之後則讓 WAF、API 和其他適用工具自動強制執行。

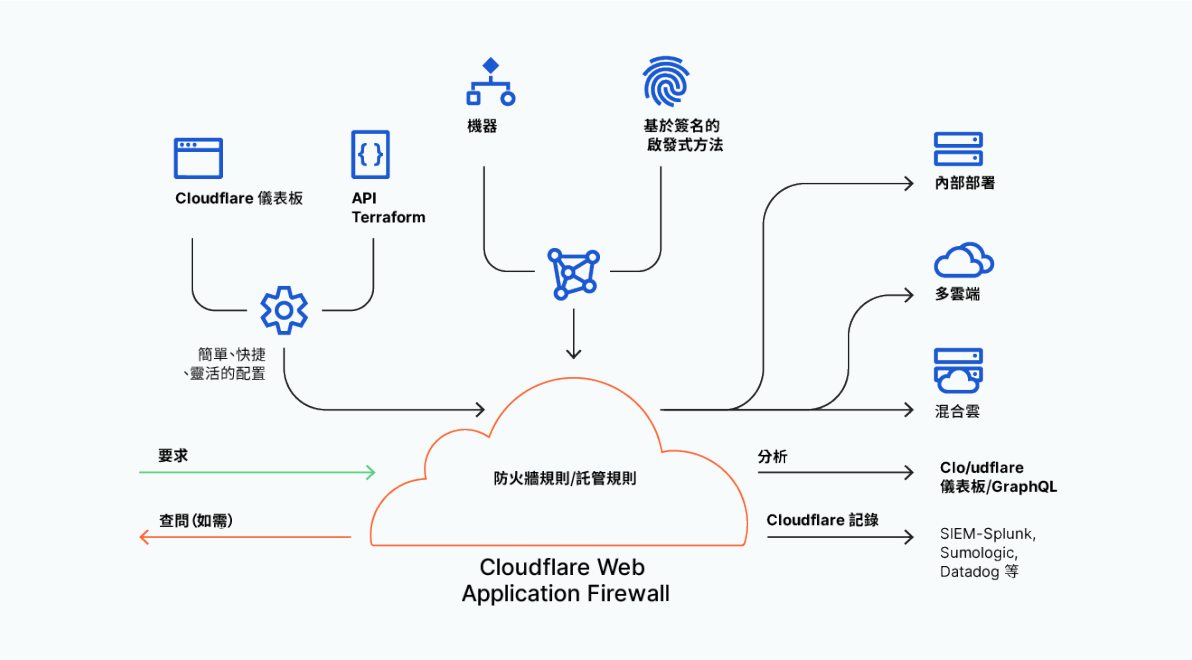


特定針對個別攻擊的策略

由於應用程式面臨許多不同類型的安全風險，有必要採取數種類型的保護。以下是應用程式擁有者可以使用的一些特定針對個別攻擊的策略：

應用程式漏洞

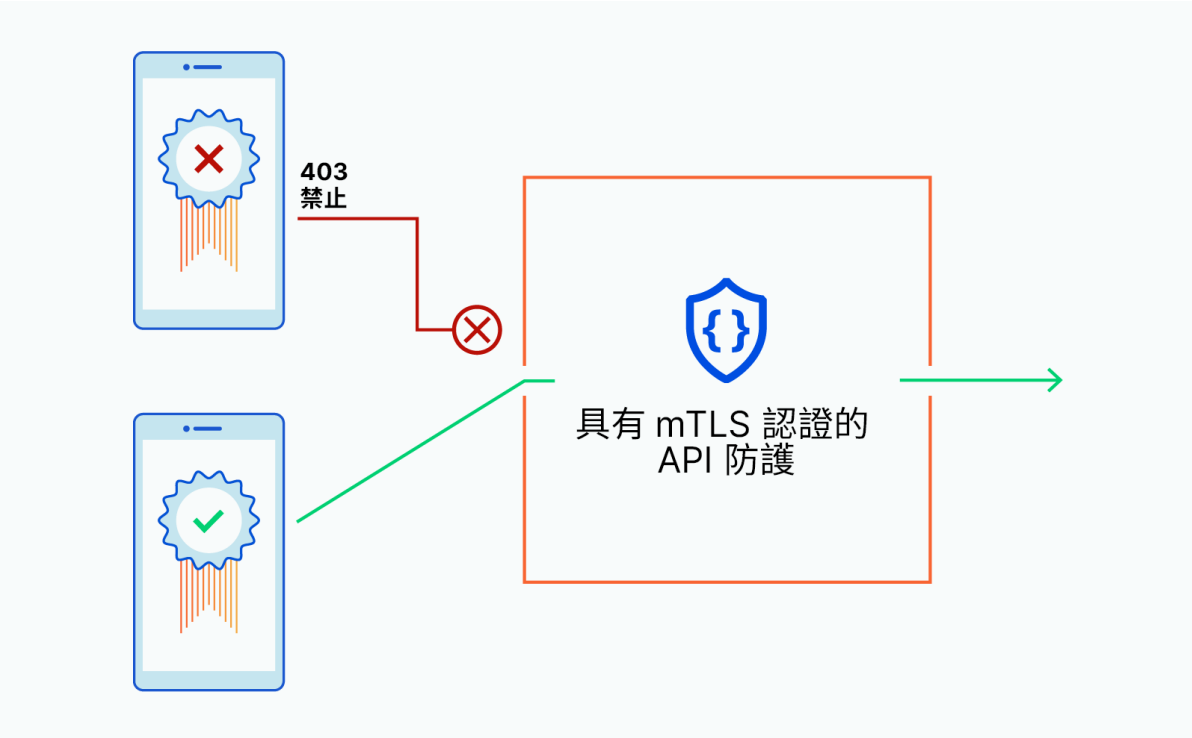
WAF：WAF 是防止攻擊者利用應用程式漏洞的最佳方式之一。WAF 針對已知攻擊技術使用一組安全性規則，以篩選掉惡意流量並防止攻擊。具有預設規則的 WAF 和部署規則快速變更的自訂化選項最為有效。這是因為這些功能可緩解許多 WAF 的其中兩個最大問題：誤判和緩慢部署規則變更。WAF 規則不小心封鎖合法網絡流量時誤判會發生。有些 WAF 需要複雜的規則設定程序，因此難以維持精確的最新清單並解除封鎖合法流量。因此，在受管理的自訂規則集之外，提供 OWASP 規則集的 WAF 可減少誤判頻率。不過，若花費太長時間部署這些新的規則，應用程式將容易受到攻擊。



資料損失預防：DLP 是用於防止資料外流 (或在未獲授權的情況下在組織之外移動資料) 的策略。DLP 工具和解決方案可監控應用程式和 API 活動，以識別潛在外洩並在發生之前停止。DLP 工具可檢查傳出的流量並與已知的資料類型比較，以判定是否為應封鎖的資料外洩。例如，DLP 工具可以識別字元字串作為使用者名稱。根據組織準備的規則，DLP 工具可以標記、停止或允許活動繼續。有些 DLP 工具可整合基於角色的存取控制 (role-based access controls，RBAC) (這規定使用者類型擁有的存取層級)，以便進一步保護資料在組織或應用程式內部的移動方式。

API 安全性風險

架構描述驗證(Schema validation)和正面表列安全模型(positive security models)：API 架構描述是描述與 API 互動之預期行為的約定。架構描述會設定基礎規則，用來允許使用者在使用 API 時可以進行的事項。OpenAPI (或 Swagger) 是最常見的架構描述格式。架構描述是良好的範本，可強制執行正面表列 API 安全。正面表列的安全模型可針對架構描述來驗證請求，僅允許符合架構描述的請求，藉此防止濫用和潛在攻擊。正面表列安全模型比反面表列安全模型更為嚴格，後者在預設情況下，除了已指示要封鎖的請求，會允許所有請求。



驗證和授權：驗證 (或確保 API 請求為合法) 和授權 (確認端點或用戶端擁有的存取層級) 也是 API 安全性的重要層面。有許多方式可以驗證和授權 API 請求。例如 Mutual Transport Layer Security (mTLS) 驗證流程，用戶端和伺服器都有用來驗證彼此身分的驗證憑證。

API 探索：「影子」API 是安全團隊可能不會注意到的 API。因為安全團隊不會監控這些 API，所以影子 API 會帶來資料外洩的可能性，或可能無法達到合規標準。API 探索工具可監控端點，以探索影子 API，藉此改善 API 管理。

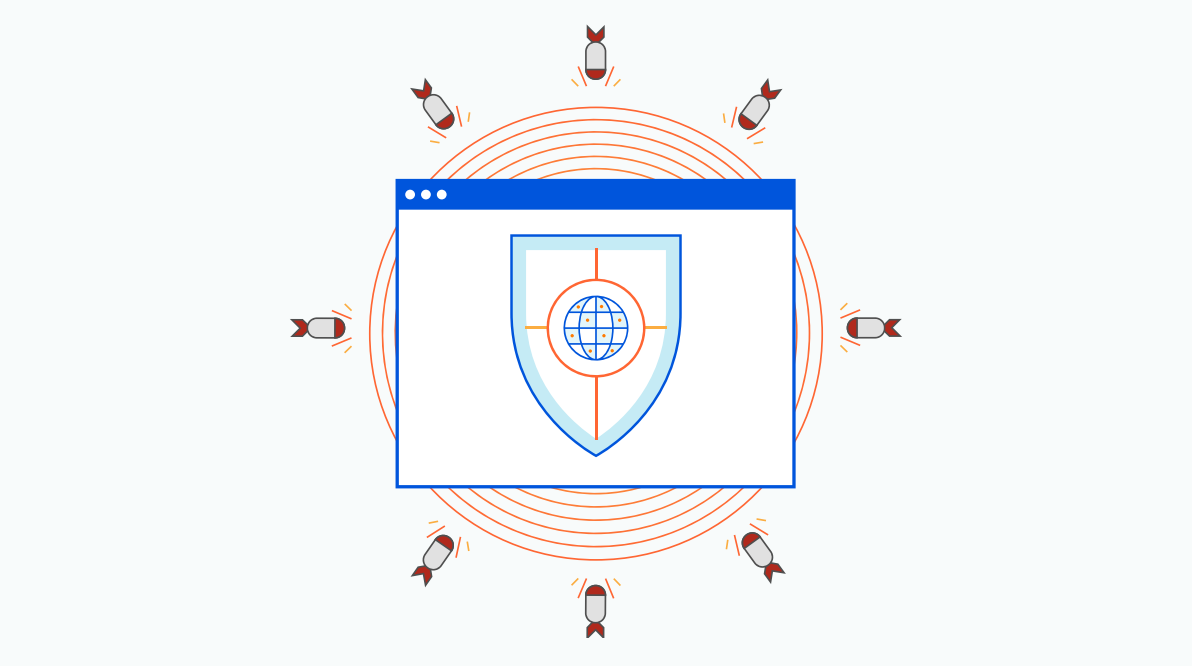
DLP：資料外流不僅會發生於傳統應用程式，也可能發生於 API。DLP 工具可用來監控傳出的 API 流量，以偵測並封鎖 API 回應中任何潛在的敏感性資料。

惡意傀儡程式

管理機器人流量需要偵測並封鎖惡意機器人，而不會封鎖善意機器人。要理解關鍵商務指標，SEO 網站，網路爬蟲等善意機器人是必要的。另一方面，惡意機器人可以破壞應用程式——執行憑證填充、內容剽竊和其他類型的攻擊。機器人管理解決方案將會分析流量，以偵測機器人活動，並判定這是善意或惡意，然後據此封鎖或允許流量。有效管理機器人需要純熟的偵測方法、能夠透過分析理解隨著時間演變的機器人流量趨勢，並且彈性使用該資料自訂機器人封鎖規則。

DDoS 攻擊

要有效防禦 DDoS 攻擊，需要最佳化緩解時間，同時不會犧牲安全性效能。一種減少緩解時間的方式是使用永遠開啟的 DDoS 保護，而不是按需求保護。與按需求保護不同，永遠開啟的緩解不會等待流量達到特定閾值再開始保護，因此可以篩選所有流量，讓緩解更快發生。來自邊緣的 DDoS 緩解讓應用程式擁有者能夠享有效能和安全性。無論攻擊源自何處，集中化保護都發生在預先定義的位置。而與集中化保護不同，來自邊緣的DDoS 緩解會在盡可能靠近攻擊來源的位置發生，以改善效能。



第三方漏洞

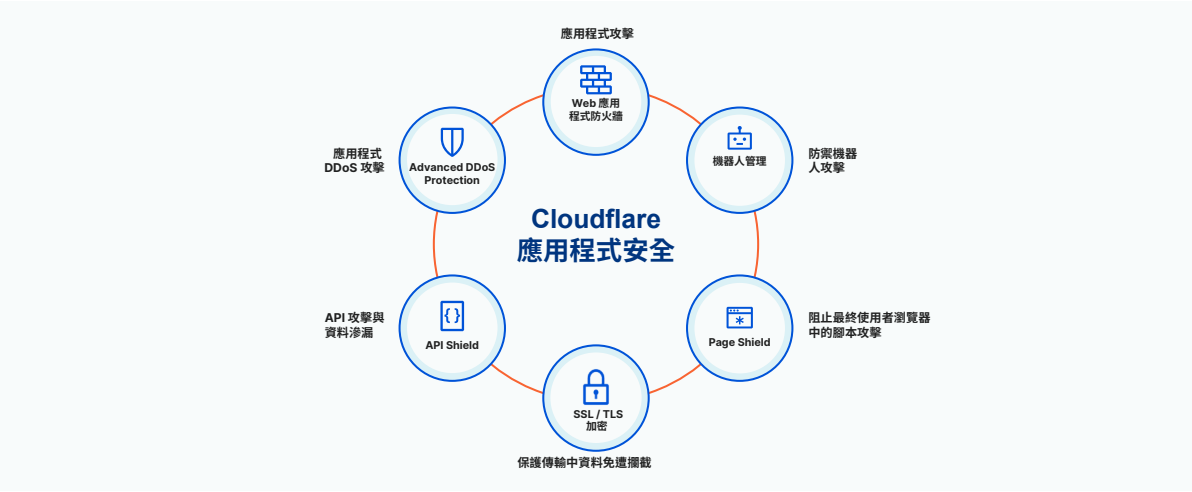
用戶端安全解決方案：因為許多網站依賴第三方，但沒有經常監控這些第三方，所以容易遭到供應鏈攻擊。在用戶端安全中，網路活動在使用者端受到保護，通常是在使用者的瀏覽器中受到保護。用戶端安全可監控第三方的變更並調查程式碼變更性質，以防禦供應鏈攻擊。例如，內容安全性政策 (Content Security Policy, CSP) 技術使用核准的資源清單，並封鎖不在清單上的任何資源以避免執行。不過，CSP 技術的缺點是並非動態。若允許清單上的資源遭到入侵並改為惡意性質，CSP 將不會封鎖惡意攻擊。幸好，有些用戶端安全產品以 CSP 的優點為基礎。有些工具能夠追蹤新的 JavaScript 相依性，並警示網站擁有者進行調查。同樣地，有些產品可以偵測網站上已知的惡意 URL 和惡意 JavaScript 服務，或警示網站擁有者調查偵測到的指令碼變更性質。

路徑攻擊

加密對於防禦路徑攻擊十分關鍵。採用安全通訊端層 (SSL)/Transport Layer Security (TLS) 加密是保護 HTTP 流量的最佳方法之一。TLS 可加密資料、驗證交換資料的雙方，並驗證資料未遭篡改。此流程可保護 Web 服務和最終使用者之間的交換，防止路徑上的攻擊。不過，有些攻擊者可以針對 SSL/TLS 運作，這就涉及了 HTTP 強制安全傳輸 (HTTP Strict Transport Security, HSTS)。HSTS 會封鎖任何來自攻擊者的不安全連線，進一步防止最終使用者遭受路徑上攻擊。

透過 Cloudflare 保護應用程式，抵禦外部威脅

使用 Cloudflare 可以防禦外部應用程式威脅。Cloudflare 邊緣網路跨越 100 多個國家中的 200 多個城市，保護數百萬個網際網路設備，以免遭到 DDoS 攻擊、應用程式漏洞、惡意機器人、API 濫用等攻擊。每個 Cloudflare 安全性服務都在我們網路的每個伺服器上執行，並從相同的全球威脅情報網中獲得資訊。



Cloudflare 應用程式安全產品包括：

- **應用程式漏洞**
  - **WAF：**Cloudflare WAF 提供分層規則集，其中包括一個定期更新的受管理規則集，可回應最新的攻擊，一個根據 OWASP 前 10 名的核心規則集，以及客戶可以快速設定和部署的自訂規則。Cloudflare WAF 在與 Cloudflare 機器人管理和 API 保護相同的 Rust 式規則引擎上操作，確保提供一致的保護。
- **API 風險**
  - **API 保護：** Cloudflare API 保護可使用用戶端憑證和架構式驗證防禦 API。API 保護使用 mTLS 驗證嘗試存取 API 的裝置/用戶端、針對 DLP 掃描傳出的流量等。
    - **DLP：**Cloudflare 也為 API 提供 DLP 功能，以封鎖包含敏感性資料的回應，例如 API 金鑰或信用卡資訊。Cloudflare DLP 功能可延伸到 API 之外，例如也能保護應用程式和裝置。
- **第三方漏洞 - 瀏覽器供應鏈攻擊**
  - **頁面保護：**指令碼監控屬於 Cloudflare 頁面保護的一部分，隨著時間記錄了網站的 JavaScript 相依性，並警示組織調查所顯示的變更或新的相依性。
- **機器人攻擊**
  - **機器人管理：** Cloudflare 機器人管理使用機器學習、行為分析和全域資料，以封鎖惡意機器人。使用機器人分析可理解流量模式並透過自訂規則和允許清單微調存取權限。
- **DDoS 攻擊**
  - **DDoS：**藉由每天平均封鎖 870 億個威脅的 90 Tbps 網路，Cloudflare DDoS 緩解防禦了來自邊緣的最大攻擊。
- **加密**
  - **Cloudflare 免費 SSL/TLS：**透過 Cloudflare 免費 SSL/TLS，您可以加密網路流量，以保護應用程式。Cloudflare SSL 也支援 HSTS 通訊協定，以提供額外的保護。

若要進一步瞭解，請至 https://www.cloudflare.com/zh-tw/security。