CLOUDFLARE

2025 年

Cloudflare 趨勢觀察報告

大規模復原能力

前言作者：MICHELLE ZATLYN

我們生活在一個前所未有的時代。技術正以驚人的速度發展。

從充滿前景與恐慌的生成式 AI 爆炸性增長，到日益無所不在的網路威脅，從超級互連世界的新矛盾，到對當地社會和全球經濟的影響，唯一不變的似乎是做出改變。遊戲規則不斷變化，如果我們的手冊不持續完善，很快就會過時。

正因為如此，推出創始版 ***Cloudflare 趨勢觀察報告*** 讓我備感自豪：這是一份年度報告，概述了網路安全趨勢和調查結果，這對於制定適合您的整體方案至關重要。

Cloudflare 為全球 20% 的網站提供保護，平均每天封鎖超過 2,270 億次網路威脅。這為我們提供了一個非常有趣的優勢點。我們看到的不僅僅是資料，更是模式、行為和轉折點，這些都預示著世界的前進方向。

我們已知的事實：AI 驅動的威脅需要採用 AI 技術提供支援的防禦。Zero Trust 必須成為標準。後量子就緒程度不是明天的問題，而要立足當下。而且，所有這一切都需要高層的參與和認可。**復原能力並非可有可無：它至關重要。**

Cloudflare 趨勢觀察報告旨在提供對影響網路安全情勢之因素的深入解析，以協助全球各種規模的企業、政府和個人做出明智的決策，以實現復原能力最佳化。

我們的使命是協助構建更好的網際網路，實現此目標從協助您取得成功開始。

Michelle Zatlyn
Cloudflare 共同創辦人
暨總裁

報告摘要

2025 年，大規模復原能力不再是選項，而是檢驗領導力的關鍵指標。

隨著數位威脅日趨複雜，地緣政治動盪加劇，企業的每一個環節——財務、營運、合規性以及聲譽——都面臨著更高的暴露風險。AI 驅動的攻擊、不斷變化的監管框架以及持續擴張的數位生態系統，都需要高階管理層採取協調一致的應對措施。

《2025 年 Cloudflare 趨勢觀察報告》重點介紹了五個關鍵隱憂，復原能力必須內建於其中，而非事後附加。這些關鍵隱憂共同揭示了高階管理團隊的全新使命：將復原能力大規模嵌入企業營運、創新與成長的核心。

精明的企業領導者已洞察到一個明顯的轉變：復原能力不再只是單一部門的責任，而是已成為整個高階管理層共同的戰略優先事項。頂尖的企業正在從被動防禦轉向主動、以情報為導向且具擴展性的技術環境，並在整個企業範圍內進行整合。將復原能力視為高階管理層的共同責任以及成長驅動力（而非僅是防護措施）的企業，將最有可能在這個日益動盪的世界中占據領導地位。

本報告重點介紹了 Cloudflare 致力於建立一個安全、高效且具復原能力的大規模數位生態系統，讓各種規模的企業都能在發生中斷時保持復原能力，並在全球範圍內自信營運。

五個關鍵隱憂

復原能力必須內建於系統之中，而非事後附加。

1

AI 支援的威脅和內部人員風險

需要技術長密切協作，因為攻擊者現在使用 AI 自動執行攻擊並擴大攻擊規模，速度超過傳統防禦的回應能力。AI 驅動的威脅必須以 AI 支援的防禦來應對，以實現即時因應。將這些功能自動化不僅能擴大防護範圍，還能讓組織在不影響業務速度的前提下擴展防禦規模。

2

Zero Trust、身分保護和雲端複雜性

需要 CIO 領導力，因為公司正從基於周邊的安全模式轉向以身分為優先的框架。Zero Trust 已成為可擴展之雲端原生風險管理的事實標準，且可確保分散式系統中的可用性、可見性與控制力。

3

復原能力對於 CFO 與 CRO 而言已不再可有可無

隨著第三方風險增加和監管框架擴展，財務與風險領導者必須確保其投資不僅僅限於緩解威脅，還應推動營運連續性、合規自動化及可擴展治理。此層級的復原能力必須是主動式、內嵌且具成本效益的，而不是一堆拼湊起來的單點解決方案。

4

資料隱私權和後量子安全準備

需要 CPO 提早介入。隨著量子運算即將破解傳統加密技術，需要立即採取具未來性的資料保護措施。領導者必須加速採用後量子加密，以便保護長期儲存的資料，並滿足不斷演變的監管要求。

5

地緣政治風險和針對性網路行動

需要 CEO 與董事會直接參與。隨著國家支援的攻擊活動越來越多地針對企業領導層、供應鏈及全球營運，企業復原能力必須提升至最高層級——由即時情報、高階主管準備度及跨境協調提供支援。

「AI 驅動的攻擊、不斷變化的監管框架以及持續擴張的數位生態系統，都需要**高階管理層採取協調一致的應對措施。**」

目錄

1

勢均力敵：在對抗性 AI 時代保護企業

勢均力敵：在對抗性 AI 時代保護企業

AI 驅動的網路威脅正以前所未有的速度發展，使得傳統的安全方法變得無效。現在，攻擊者使用 AI 來自動化攻擊、逃避偵測，並且利用漏洞的速度比組織做出回應的速度更快。從被動防禦轉變為主動、AI 驅動的網路安全不再可有可無，而是勢在必行。

AI 支援的攻擊已經對業務造成實際影響。74% 的 IT 安全專業人員反映，AI 驅動的威脅正在嚴重影響他們的組織[1]。深度偽造詐騙（例如，詐騙性視訊通話）已造成數百萬美元的損失，其中澳洲一起案件導致 2,500 萬澳元的盜竊[2]。AI 產生的網路釣魚攻擊變得越來越有說服力，而 AI 增強的惡意程式碼則會適應以規避傳統防禦。

除了直接攻擊，AI 還助長了錯誤資訊活動、資料中毒和模型操縱，從而可能會損害 AI 驅動的系統。

攻擊者生產力提升，會給安全團隊帶來巨大壓力

許多支援 AI 的工具可能無法解鎖突破性的攻擊技術，但這些工具可協助對手改善生產力、效率和攻擊量。這些工具可加速製作網路釣魚電子郵件等任務，以及使用「黑暗聊天機器人」協助編寫惡意程式碼。

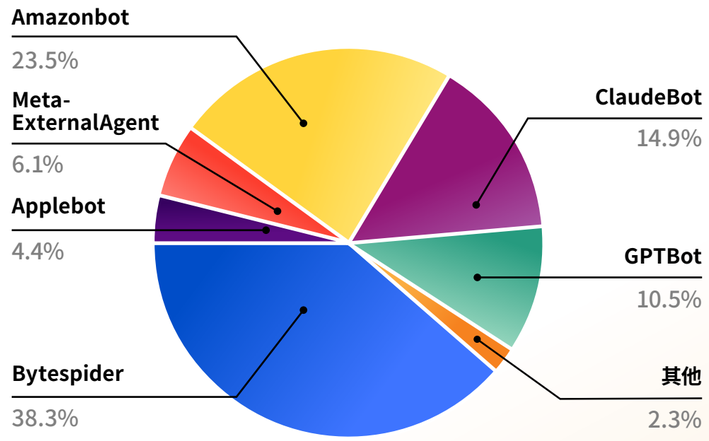
這意味著組織將開始面臨更大規模、更複雜的攻擊，通常使用現代攻擊方法。隨著攻擊量的增加，手動安全程序（例如，分類網路釣魚電子郵件和手動調整偵測以阻止最新威脅）肯定會變得捉襟見肘。

AI 剽竊威脅數位內容創作者

AI 模型需要資料來進行訓練，並且許多 AI 公司透過自動化 Web 剽竊來收集該資訊。實際上，Cloudflare 在我們網路上處理的所有機器人流量中，AI 網路爬蟲已經佔了 2%[3]。

AI 衍生的內容可轉移網站的流量和互動，嚴重損害依賴線上內容和廣告營收的組織。反對的聲音越來越大。2025 年 2 月，教育公司 Chegg 起訴 Google 損害其 AI 流量，英國創意產業發起「公平公正」活動，反對未經許可使用內容[4]。

依應用程式層流量佔比的主要 AI 網路爬蟲



Cloudflare 在 2024 年觀察到的 AI 網路爬蟲流量幾乎全部 **(98%)** 都**源自六間公司**[5]。

對於嚴重依賴於發布數位內容或數位廣告的組織來說，**AI 剽竊者是一種關乎生死存亡的威脅。**

合成身分詐欺擾亂關鍵產業

AI 助長了合成身分詐欺 (SIF) 的興起，罪犯透過混合真實和虛假資料來繞過傳統驗證系統，從而建立超逼真的身分。AI 產生的個人詳細資訊、深度偽造和自動化認證填充使這些身分更難以偵測，並為金融服務、醫療保健和政府機構等遭受嚴重攻擊的產業帶來重大風險。

與傳統詐騙不同，SIF 經常被忽視，因為它缺乏直接的受害者，允許詐騙者建立信用記錄並執行大規模詐騙。

AI 加劇了內部人員威脅

遠端工作和雲端採用擴大了內部人員威脅的攻擊面，使其更難以偵測。超過一半的組織反映去年經歷了內部人員威脅，8% 的組織遭遇了 20 多起事件[6]。

現在，AI 放大了這一挑戰，為內部人員提供了強大的工具來逃避偵測。支援 AI 的網路釣魚、深度偽造詐騙和自動化社交工程攻擊，可在幾秒鐘內產生令人信服的內容感知訊息，使詐騙更容易且攻擊更頻繁[7]。

並非所有內部人員威脅都是蓄意攻擊。Verizon 的 2024 DBIR 發現，68% 的資料外洩是人為因素造成的，例如，個人受社交工程騙局的欺騙或犯錯[8]。AI 輔助的魚叉式網路釣魚利用這些錯誤，以近乎完美的準確性模仿真實的同事或高管，來誘騙員工共用認證、核准交易或暴露敏感性資料。

組織必須部署行為分析、即時監控和異常偵測，才能在風險升級之前發現此類風險。現在，採用 AI 技術的安全自動化對於應對 AI 驅動型威脅的速度和規模至關重要。

AI 驅動的機器人重塑網路安全環境

AI 驅動的機器人正不斷增加攻擊複雜性和風險暴露。2024 年，Cloudflare 觀察到的所有應用程式流量中，有 28% 來自機器人，這一數字在過去四年一直穩定在 30% 左右。雖然機器人可用於合法用途，例如，客服自動化和搜尋引擎索引，但絕大多數 (93%) 未經驗證且可能存在惡意[9]。

關鍵的轉變是 AI 支援的機器人能夠以前所未有的效率，進行大規模的自動化攻擊。現在，攻擊者使用機器人來執行認證填充、發起分散式阻斷服務 (DDoS) 攻擊、剽竊敏感性資料，並以機器的速度執行詐騙。AI 模型透過產生逼真的網路釣魚嘗試、繞過傳統的 CAPTCHA，以及透過適應性行為逃避偵測，來增強這些功能。

現在，採用 AI 技術的安全自動化對於應對 AI 驅動型威脅的速度和規模至關重要。

Cloudflare 觀察到的所有應用程式流量中，有

28% 來自機器人

高層面臨的問題

構建 AI 驅動的防禦能力

為了提前應對 AI 驅動的威脅，組織需要採用主動方法來即時預防和緩解這些威脅。
以下是公司高層領導者在評估其組織就緒程度時可提出的幾個問題。

問題一

我們是否正在使用 AI 來推動全面的安全可觀測性？

我們是否在單一介面統一記錄、分析、警示和取證，以識別風險及其根本原因？

問題二

我們是否正在利用 AI 驅動的安全性來即時偵測和消除威脅？

我們是否使用 AI 支援的偵測來分析龐大的資料集、識別異常狀況，並自動回應新興威脅？

問題三

我們在抵禦 AI 支援的網路釣魚、深度偽造和惡意程式碼的保護程度如何？

我們是否部署了 AI 驅動的偵測、防網路釣魚驗證和適應性安全控制，來應對不斷發展的攻擊？

問題四

我們是否正在保護我們的專有資料免受 AI 剽竊者和自動化威脅的侵害？

我們是否部署了機器人管理、API 驗證和數位浮水印來防止資料竊取和利用？

問題五

我們是否正在利用 AI 驅動的行為分析來即時偵測內部人員威脅？

我們是否在持續分析使用者行為，包括存取模式、權限提升和資料外流嘗試？

高階主管觀點

AI 資料安全的新防護機制

Dane Knecht
Cloudflare 技術長

保護 AI 時代的資料：信任、存取和可見度

當今組織最緊迫的痛點是資料存取，具體而言，就是如何在 AI 工具日益普及的企業中管理和保護資料。隨著生成式 AI 嵌入工作流程，挑戰不再只是對威脅做出回應，更要防止對敏感性資料進行有風險或未經授權的存取。

這給董事會和高層帶來了緊迫的問題。我們如何安全地授予工具對企業資料的存取權？我們如何確保一個看似無害的 AI 附加元件不是資料外流的閘道？商業方案和聲譽的影響是真實存在的，並且與日俱增。

我們的不足之處：影子 AI 和盲目的治理漏洞

一個主要的盲點是，AI 工具在整個企業中不受控制的傳播。員工遠在正式政策出台之前採用 AI，但往往並沒有意識到風險。這些「影子 AI」部署會迴避傳統審查，從而產生看不見的攻擊面和新的合規性風險。

很少有組織繪製使用 AI 的地圖。若沒有這種可見度，幾乎無法管理資料暴露或有效回應事件。

後續方案：主動控制和增強的監管審查

在接下來的 12–18 個月內，企業安全性將從被動式威脅偵測轉變為主動式 AI 存取和使用治理。監管審查將更加嚴格，這要求透明度、營運監督和強大的資料保護做法。

快速行動的組織（透過組建跨職能治理團隊、定義 AI 使用原則，以及為工具和使用者實作存取控制）將降低風險，並將自己定位為領導者。

復原能力的未來不僅僅是發現威脅，更是控制 AI 接觸資料的方式和位置。

「員工遠在**正式政策出台之前採用 AI**，但往往並沒有意識到風險。」

2

超越邊界：Zero Trust、身分和新的安全前沿

超越邊界：Zero Trust、身分和新的安全前沿

轉向多雲端環境、SaaS 平台和 API 驅動的架構，造成了碎片化的安全環境，其中錯誤設定、身分風險和影子 IT 讓企業面臨日益增加的網路威脅。在這種環境中，Zero Trust 安全性已經取代了過時的基於週邊的模型，成為透過以身分為中心的持續驗證方法，來保護雲端應用程式、工作負載和資料的基礎。

為了跟上步伐，組織必須在雲端和 SaaS 平台中強制實施 Zero Trust 原則。

Zero Trust 取代傳統的 VPN

現在，威脅執行者會利用零時差漏洞和暴力密碼破解嘗試來主動攻擊 VPN 提供者，以便存取網路[10]。隨著網路週邊崩潰，組織正在轉向以身分為中心的安全性，在雲端工作負載和 SaaS 應用程式中強制實施持續驗證、最低權限存取和關聯內容驗證。

Zero Trust 網路存取 (ZTNA) 現在變得至關重要，取代了讓企業容易遭受認證式攻擊、橫向移動和內部人員威脅的傳統 VPN。若沒有 Zero Trust，企業將面臨未經授權存取、認證洩露和供應鏈漏洞的風險。

API：新興的攻擊手段

現在有 60% 的網際網路流量以 API 為基礎，因此不安全的 API 已成為攻擊者的主要目標[11]。許多組織未能追蹤和保護 API，使其容易遭受資料外流、認證濫用和資料隱碼攻擊。Cloudflare 以機器學習為基礎的分析發現，組織少報了四倍的 API 端點，造成了嚴重的安全盲點[12]。

為了緩解風險，企業必須採用自動化 API 探索、驗證實施和 AI 驅動的異常偵測，以防止違規和資料外洩。

Cloudflare 以機器學習為基礎的分析發現，**組織少報了四倍的 API 端點**

影子 IT 和未受管雲端服務會加劇風險

快速採用未經批准的雲端服務，使得 IT 團隊越來越難以有效地監控和保護雲端環境。員工經常使用未經核准的協作工具，從而暴露敏感性資料，並繞過公司安全性原則。

雲端存取安全性代理程式 (CASB)、AI 支援的探索工具和自動化原則實施，現在對於獲得即時可見度、確保合規性和防止未經授權的資料暴露至關重要。

以身分為中心的安全性：密碼的終結

隨著網路威脅變得越來越複雜，身分仍是主要的攻擊手段。2024 年第一季，Cisco 25% 的事件回應工作與使用者接受詐騙性多重要素驗證 (MFA) 推送通知有關[13]。認證泄露亦會導致嚴重的資料外洩，例如，針對包括 Santander Group、Ticketmaster 和 Advanced Auto Parts 在內的至少 160 家 Snowflake 客戶[14]。

越來越多的網路罪犯繞過 MFA、劫持作用中工作階段並竊取認證，從而使企業面臨廣泛的外洩和帳戶盜用。

挑戰：

- **認證重複使用讓企業面臨風險** – 在所有人類登入嘗試中，有 46% 涉及認證洩露，在企業級組織中，這一數據上升至 60%[15]。攻擊者自動執行認證填充，從而輕鬆獲得對企業系統的存取權。
- **自動化認證攻擊正在迅速擴展** – 在使用外洩認證的登入嘗試中，有 94% 來自機器人，每秒要測試數千個被盜密碼[16]。若沒有即時機器人緩解和適應性驗證，組織仍然很容易遭受大規模外洩。
- **密碼不足** – 靜態密碼，甚至基本的 MFA 方法在抵禦現代威脅 (包括 MFA 繞過、工作階段劫持和防網路釣魚認證盜竊) 方面越來越無效。為了應對這些風險，組織必須採用無密碼驗證、強制執行 Zero Trust 存取控制，並部署符合 FIDO2 規範的安全金鑰，來消除對靜態認證的依賴。

在人類登入嘗試中，有

46% 涉及**認證洩露**

在使用外洩認證的登入嘗試中，有

94% 來自機器人，**每秒要測試數千個被盜密碼**

高層面臨的問題

保護雲端並重新考慮驗證

隨著雲端採用加速，組織必須重新考慮安全性和驗證，以防禦不斷演變的威脅。Zero Trust 方法、AI 驅動的可見度和強大的身分保護，對於保護雲端服務、SaaS應用程式和 API 至關重要。**透過以下問題來確定您的組織應對這些挑戰的主動程度：**

問題一

我們是否在雲端、SaaS 應用程式和 API 中強制執行 Zero Trust 安全性？

我們是否在所有環境中提供持續驗證、最低權限存取和基於風險的驗證？

問題二

我們是否全面深入解析影子 IT 和未受管雲端服務？

我們是否使用 AI 驅動的探索工具，來偵測未經授權的應用程式並強制執行安全性原則？

問題三

我們的 API 是否得到保護，以防止未經授權的存取和資料外洩？

我們是否正在實作自動化 API 探索、驗證控制和 AI 驅動的異常偵測？

問題四

我們是否已消除驗證策略中基於密碼的漏洞？

我們是否正在採用無密碼驗證、防網路釣魚的 MFA 和自適應身分保護？

問題五

我們是否準備好偵測並回應自動化認證攻擊？

我們能否部署 AI 驅動的機器人緩解、行為分析和自動化認證撤銷，來防止未經授權的存取？

高階主管觀點

Zero Trust 打造具備復原能力的未來

Corey Mahan
Cloudflare 產品管理副總裁

目前，組織面臨的最大挑戰是平衡安全性與可用性。混合式工作勢在必行，雲端採用正在加速，並且使用者希望能夠順暢存取，無論他們身在何處或使用什麼裝置。但傳統架構已無法滿足需求。我們看到太多企業依賴於無法很好擴展的拼湊式單點解決方案，從而導致服務中斷、延遲和使用者失望。

高階主管提出了一個關鍵問題：如何在不減慢業務速度的情況下提供安全性存取？正是這種壓力使得 Zero Trust 脫穎而出，不僅作為一種安全模型，更是業務推動者。

常見缺陷

許多組織一開始有正確的意圖，但後來卻陷入困境。一個常見的缺陷是認為購買「Zero Trust 解決方案」就等同於實作策略。事實並非如此。Zero Trust 是一種心態和架構轉變。

另一個問題是，假設統一意味著整合 — 許多所謂的平台只是拼湊在一起的產品，不共用資料或原則，甚至不共用後端。這會產生盲點，尤其是在雲端 API、DevOps 管道和 AI 應用程式等現代環境中。

然後是影子 IT 和影子 AI，這是員工正在使用但 IT 團隊卻不知道的工具，從而造成嚴重的治理漏洞。

下一步行動（12–18 個月）

在接下來一年左右的時間，我們將看到 Zero Trust 從孤立的控制演進為涵蓋整個企業的基礎層。重心將從單獨的安全、遠端存取管理，轉變為在所有環境中統一身分、資料和流量原則。領導者已經在轉向設計具有彈性、預設為全域性、自動回應，並提供即時可見度的平台。這才是真正的價值所在：不僅能降低風險，還能實現敏捷性。

那些取得領先地位的組織，會將 Zero Trust 嵌入其數位基礎，從而使其成為他們安全地構建、擴展和創新方式的一部分。

「一個**常見的缺陷**是認為購買「Zero Trust 解決方案」就等同於實作策略。」

3

更強大，而不僅僅是更安全：在基礎架構、生態系統和監督中擴展保護

更強大，而不僅僅是更安全：在基礎架構、生態系統和監督中擴展保護

在網路、供應鏈與合規性架構之間構建復原能力，對於維持營運完整性和競爭優勢至關重要。

然而，如今的網路威脅（如 DDoS 攻擊）速度更快、規模更大且更複雜，超出了傳統防禦的範圍。與此同時，數位供應鏈暴露了隱藏的漏洞，而監管環境亦變得越來越苛刻和分散。

為了保持競爭力，組織必須將網路安全從 IT 問題重新定義為業務復原能力策略，這種策略可跨基礎架構、生態系統和監督進行擴展。

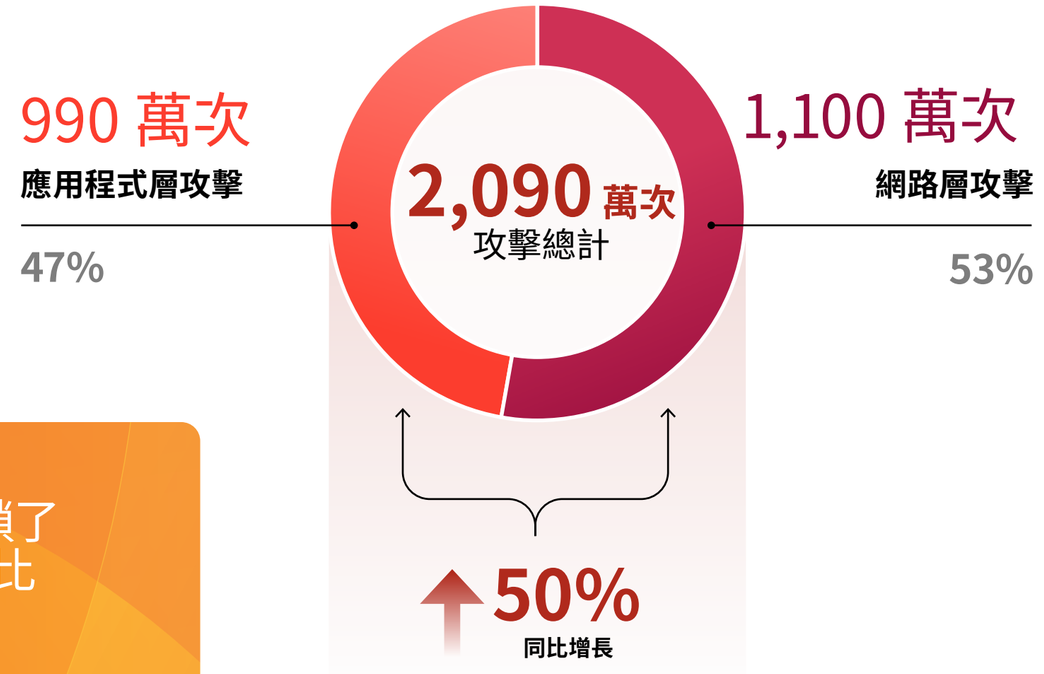
DDoS 攻擊的規模和複雜度急劇上升

DDoS 攻擊已演進為網路罪犯、駭客和民族國家用於破壞營運並造成監管和聲譽影響的精確工具。DDoS 攻擊正在削弱各行各業的企業。2024 年，Cloudflare 封鎖了 2,090 萬次 DDoS 攻擊，比 2023 年增長了 50%[17]。

DDoS 攻擊的規模和複雜程度不斷升級，攻擊者利用殭屍網路、IoT 裝置和 AI 驅動的自動化，對關鍵數位服務發起持續性、高影響力的攻擊。

2024 年，Cloudflare 封鎖了 2,090 萬次 DDoS 攻擊，比 2023 年增長了 50%

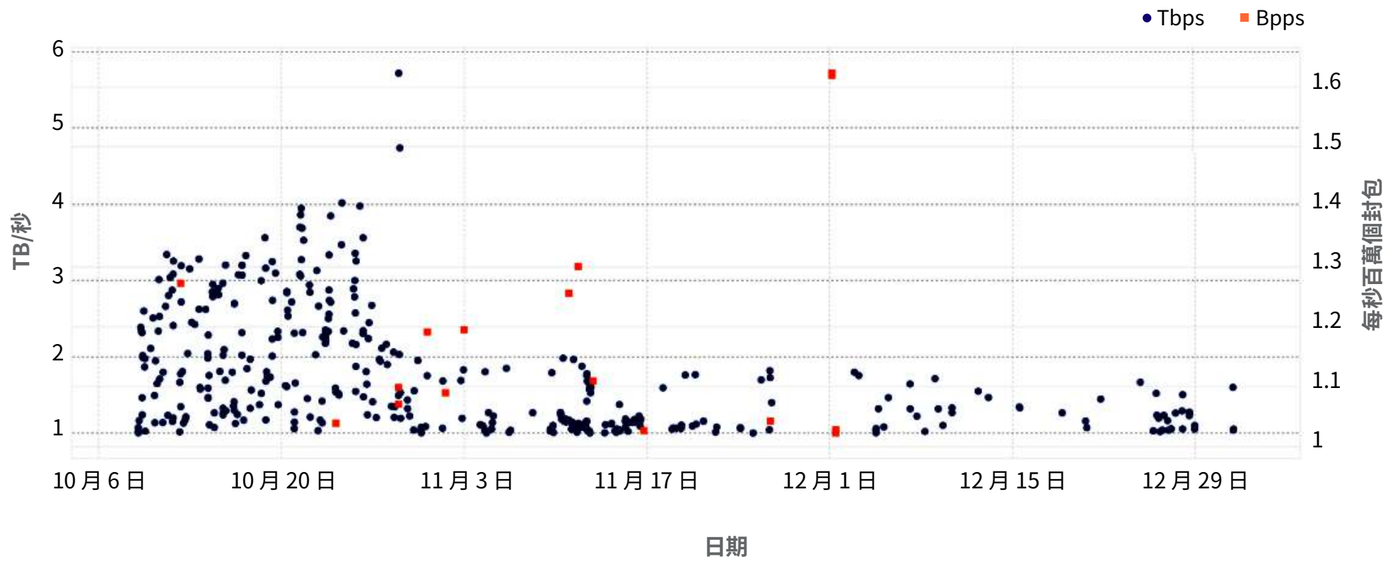
2024 年 DDoS 攻擊



超流量 DDoS 攻擊的興起

2024 年第四季

在 2024 年第四季，超流量網路層攻擊以前所未有的水平激增。超過 1 Tbps 的攻擊數量，以 1,885% 的季度環比增長率激增；而每秒超過 1 億個封包 (pps) 的攻擊數量，以 175% 的季度環比增長率激增。值得注意的是，在每秒超過 1 億個封包 (pps) 的攻擊中，有 16% 還超過 10 億 pps，這凸顯了現代 DDoS 威脅的強度和規模不斷增長[18]。



Cloudflare 資料顯示，企業級組織平均使用**至少 20 個第三方指令碼**

不斷升級的供應鏈攻擊

根據世界經濟論壇的報告，54% 的大型企業將第三方風險管理視為其最大的網路復原能力挑戰[19]。針對軟體供應鏈、雲端平台和第三方整合的攻擊急劇上升；2024 年，15% 的資料外洩涉及第三方[20]。

雪上加霜的是，風險越來越集中在少數幾個居主導地位的雲端提供者上。其中一個提供者的單一漏洞或服務中斷，可能會波及整個產業，2024 年的重大 IT 服務中斷就是明證，這造成了數十億美元的損失，並暴露了超連接數位生態系統的脆弱性。這些事件有力地提醒人們，在當今相互依存的環境中，單一失敗點可能導致整個營運陷入停滯。

一個特別容易受到攻擊的領域是用戶端側攻擊，企業經常依賴於第三方指令碼來加速 Web 應用程式開發。這些指令碼是源自外部伺服器的內嵌程式碼，通常為 JavaScript。

雖然這些指令碼提升了效率，但它們也會造成嚴重的安全漏洞：與外部功能的每一次連線都會增加基於瀏覽器的供應鏈攻擊風險。

Cloudflare 資料顯示，企業級組織平均使用至少 20 個第三方指令碼，而有些組織在不知情的情況下使用了數十萬個，每個都代表著一個潛在的攻擊者入口點。

一個大型電子商務組織在其網站上附接了超過 340,000 個第三方指令碼[21]。

歐盟《網路復原能力法案》和《支付卡產業資料安全標準》(PCI DSS 4.0) 等法規有助於解決供應鏈安全問題，但強制執行仍是一項挑戰。

網路安全法規激增

網路安全法規正在快速擴展，對企業增強安全性、透明度和事件報告提出了更高的要求。美國證券交易委員會 (SEC) 現在要求上市公司披露重大網路安全事件，並詳細說明其風險管理策略。歐盟一般資料保護規定 (GDPR) 仍是最嚴格的資料隱私權法律之一，對違規行為處以高達全球營收 4% 的處罰。澳洲審慎監管局 (APRA) CPS 234 要求金融機構必須採取穩健的資訊安全措施，而歐盟的《數位營運彈性法案》(DORA) 則為金融業設定統一的網路安全標準。

換句話說，合規性不再是事後的想法。成功應對這一情勢的組織將合規性嵌入到其營運中，從而利用自動化來精簡報告，並確保與不斷演變的法規持續保持一致。

合規自動化升級

隨著組織面臨越來越複雜的監管和營運風險，合規自動化正成為一種重要趨勢。由於目前僅在美國就已執行或提議超過 52 項網路事件報告要求，而且 GDPR、DORA 和 PCI DSS 4.0 等全球框架的範圍也在不斷擴大，手動合規性程序不再具有永續性[22]。一項 Deloitte 問卷調查顯示，由於監管碎片化和即時回應需求，62% 的全球組織計劃增加對合規自動化的投資[23]。

為了在不犧牲效能的情況下滿足管轄區資料要求，公司正在採用策略性資料當地語系化，透過區域節點來路由流量，並部署自動化稽核工具來驗證合規性。與此同時，合規性與安全性之間的界限越來越模糊 — 企業正在實施整合式架構，以協調威脅偵測、原則強制實施和稽核准備。

這種融合讓企業能夠降低風險、加速回應監管變化，以及擴展跨邊界治理。實現合規自動化和運作化的組織將獲得策略性優勢，從而加速進入受監管市場、增強客戶信任度，並將財務和聲譽風險降至最低。

監管環境不斷成長

全球網路安全和資料保護監管框架持續快速發展，現在，組織必須在不同管轄區應對複雜的 Web 合規性要求。

例如：

SEC 網路安全規則

美國 SEC 對上市公司實施了全面的網路安全披露要求。這些規則要求及時報告重大安全事件，並詳細披露風險管理策略、治理和專業知識的相關資訊。

NIS2

歐盟的 NIS2 指令對 18 個關鍵部門設定了更嚴格的安全要求。它規定了復原能力、風險管理、事件回應和報告措施，並加強了對不合規的監督和處罰。

APRA CPS 234

澳洲審慎監管局的《CPS 234 資訊安全標準》要求金融機構保持穩健的資訊安全功能，並與其資訊資產面臨的威脅規模和程度相稱。

DORA

DORA 代表歐洲在金融業數位營運復原能力方面的綜合性方法。它針對支援金融實體營運的網路和資訊系統的安全性，建立了統一的要求。

高層面臨的問題

重新構想持續性與合規性

在大規模 DDoS 攻擊、不透明的供應鏈和複雜的全球法規所塑造的威脅環境中，切實地復原能力不僅僅是防禦。這意味著設計的系統能夠在壓力下持續運作，並將合規性同時視為保障措施和策略性推動因素。**以下五個問題可協助 CXO 評估其組織在承受和適應中斷方面的就緒程度。**

問題一

我們的基礎架構能否承受大規模 DDoS 攻擊，並在壓力下維持正常運作時間？

緩解能力應超過尖峰合法流量和記錄的最大型攻擊。具有復原能力的組織會實作地理上備援的基礎架構與合規性容錯移轉計畫，並定期測試復原程序，來確保正常運作時間和監管一致性。

問題二

我們是否可即時地深入解析最關鍵的第三方相依項？

供應鏈漏洞是導致安全事件的主要原因。具有前瞻性的組織會持續監控外部廠商和服務，強制執行合約安全性要求，並將第三方風險深入解析整合至更廣泛的治理程序中。

問題三

我們是否已自動化合規工作流程，以跟上全球法規的步伐？

隨著許多監管框架迅速演變，手動的合規方法無法進行擴展。高效能企業利用自動化稽核、即時監控和可感知管轄區的資料路由，來保持持續一致性並減少開銷。

問題四

我們的安全性與合規性功能是否完全整合？

孤立的團隊會造成效率低下和差距。統一平台可讓威脅偵測與監管報告保持一致，精簡了稽核程序、改善了可見度並全面降低了風險。

問題五

我們是否測試了從事件偵測到復原和報告的完整復原能力狀態？

積極主動的組織會制定手冊，將技術控制與監管要求關聯，定期模擬中斷，並調整合規性架構，以在管轄區內擴展。

高階主管觀點

新的就緒程度規則

Emily Hancock
Cloudflare 隱私長

保障未來：監管、風險和就緒程度

網路安全監管正在進入一個要求更嚴格、審查更細緻、問責更廣泛的新時代。從 SEC 的強制性事件披露，到 GDPR 嚴厲的隱私權處罰，再到 DORA 和 APRA CPS 234 等新標準，全球監管機構不斷提高對資料保護、營運連續性和透明度的期望。對於行政團隊而言，合規性不再只是一項法律義務，更是一項策略性優先任務。

與此同時，新技術和不斷演進的威脅模型正在挑戰傳統的安全性方法。隨著創新加速，監管機構和利害關係人更加關注長期風險管理，特別是在敏感性資料方面。組織必須證明他們不僅可以保護今天的資產，還可保護將支撐未來數位信任的資料和系統。

我們的不足之處：誤解和被忽視的差距

許多組織仍然將安全性與合規性視為孤立的功能，由技術團隊管理，而無需跨部門協調。這會產生盲點，在瞭解敏感性資料所在位置、如何套用加密，以及第三方系統中漏洞所在位置時尤其如此。

如果沒有明確的清單和治理框架，組織可能會同時落後於監管機構和攻擊者。

另一個差距是最大限度地減少資料。很多時候，企業會保留不再需要的個人資料，增加風險程度，而沒有任何商業效益。嵌入將隱私納入設計的原則（在架構層級限制資料收集、自動刪除和內建控制），可以降低風險並改善監管一致性。

下一步行動：轉向嵌入式合規性

在接下來的 12–18 個月內，我們預計監管機構和標準機構將更加重視主動、可驗證的安全做法。這包括在資料治理、加密和第三方風險方面更強大的控制。企業盡早行動（透過採用整合式平台、自動化合規工作流程，以及將安全性嵌入核心營運等方式），將會降低複雜性，避免代價高昂的補救措施，並將自己定位為值得信任的領導者。

這種轉變顯而易見：必須從一開始就在設計中考慮合規性、持續性與安全性。組織將這種思維模式內化，不僅能跟上法規的發展，還能在一個要求問責制、透明度和信任的世界中發揮領導作用。

「若沒有明確的清單和治理框架，**組織可能會同時落後於監管機構和攻擊者。**」

4

破解密碼：量子時代與時俱進的隱私權

破解密碼：量子時代與時俱進的隱私權

量子運算有望為科學和產業帶來變革性進步，但它亦對數位安全性構成基礎威脅。一旦大規模量子系統成熟，它們將能夠破解廣泛用於保護網際網路安全的公開金鑰加密系統。這包括 TLS 加密、VPN、程式碼簽署和區塊鏈系統。

危險不是假設的。如今，威脅執行者已經在收集加密資料，並押注未來的量子電腦將能夠對其進行解密，這種策略被稱為「先竊取、後解密」。隨著後量子加密技術的採用加速，加密系統的可見度、自動化原則強制執行，以及清晰的遷移路徑將定義組織的就緒程度。

量子威脅已經出現

美國國家標準與技術研究院 (NIST) 警告，組織應立即採取行動，以免措手不及[24]。民族國家執行者和老練的對手正在積極收集加密流量、智慧財產權和國家機密，以供日後解密。如果不採用量子復原金鑰協定進行保護，需要保密長達十年 (或更長時間) 的通訊 (例如醫療保健記錄、軍事情報和法律合約) 已經很容易受到攻擊。

PQC 採用率激增，但差距依然存在

後量子加密技術 (PQC) 已從理論研究轉向生產實作。包括 Cloudflare在內的大型科技公司正在引領 PQC 的採用。

2024 年初，Cloudflare 報告稱，只有 3% 的 HTTPS 流量使用後量子演算法進行加密。到 2025 年 3 月，在 Cloudflare 推出預設的混合後量子 TLS，以及 Chrome、Edge 和 Firefox 的瀏覽器支援之後，這一數字達到了 38%[25]。

不過，採用情況並不均衡。大多數企業環境都處於探索或試點階段的早期，加密技術氾濫使得過渡變得複雜。企業若未能優先考慮抗量子加密，可能會落後於監管要求，並將其資料暴露於長期漏洞中。

後量子加密全球採用情況

HTTPS 要求流量中的後量子加密佔比

量子遷移策略

1

首先記錄使用加密技術的所有位置。

建立遷移專案清單，依風險和工作量進行優先排序。

立即將後量子就緒程度作為廠商評估程序的一部分。

2

在採用最新標準方面，並非所有廠商都能提供同等程度的服務。驗證廠商加密敏捷性，尤其是傳送企業網路流量的 Zero Trust 廠商。

3

首先優先考慮金鑰協定遷移。

由於存在「先竊取、後解密」的威脅，現在確保您的金鑰協定具有量子抗性有明顯的好處。廠商在轉向 TLS 1.3 以支援 X25519MLKEM768：X25519MLKEM768 方面進行了很大程度的融合：傳統橢圓曲線 X25519 與後量子 ML-KEM（基於模組晶格的金鑰封裝機制標準，FIPS 203）的混合方案。

應記錄簽章遷移，但此時不優先考慮。

對於遷移至後量子簽章的正確方法，組織仍在努力達成共識。幸運的是，後量子簽章主要用於防禦主動中間人攻擊，從而降低此遷移的優先順序。

4

加密可見度和 XDR 驅動的自動化將加速轉換

後量子遷移不僅僅關乎部署新的演算法，更要瞭解加密技術在日益龐大環境中的存在位置。這包括嵌入式系統、雲端工作負載、舊版應用程式、API 和 IoT 裝置。安全團隊使用具有深度網路和端點遙測功能的延伸偵測與回應 (XDR) 平台，能夠更好地發現過時的加密、偵測不安全的回退行為，以及自動執行補救工作流程。

廠商加密敏捷性將成為一項風險差異化因素

監管機構（例如，NIST、BSI、ANSSI）開始推薦或強制要求加密敏捷性架構。企業將越來越多地在 RFP 和供應鏈稽核中評估後量子就緒程度。然而，並非所有廠商都在同步發展。若不支援混合或量子安全加密，可能會面臨取消資格，特別是在政府、金融服務和國防部門。

高層面臨的問題

做好準備迎接量子風險

隨著攻擊者採取「先竊取、後解密」的策略，以及監管機構轉向後量子要求，組織必須立即開始準備。牽頭完成這一轉換的高階主管不僅使其基礎架構能夠適應未來的需求，還會在信任、合規性和復原能力方面獲得策略性優勢。**藉由提出以下問題，來考量您是否已為即將到來的量子風險時代做好準備：**

問題一

我們是否全面深入解析加密技術在環境中的使用位置 — 從雲端和應用程式，到嵌入式系統和第三方工具？

密碼編譯系統通常是深度嵌入的，並且記錄不充分。若沒有完整的可見度，組織可能會讓關鍵系統處於未受保護的狀態，或在不知不覺中暴露於量子時代的威脅之下。

問題二

我們是否已優先遷移至後量子金鑰協定通訊協定，特別是保護敏感性或長生命週期資料的系統？

「先竊取、後解密」的攻擊目標是必須多年保密的資料。遷移金鑰交換機制（例如 TLS 交握）是確保未來機密性的一個影響深遠且時間敏感的步驟。

問題三

我們的偵測和資產監控工具是否能夠在整個企業中，識別過時或易受量子攻擊的加密技術？

XDR、SIEM 和資產探索平台應有助於偵測加密漂移、舊版程式庫和回退通訊協定。這對於防止設定錯誤和指引遷移優先事項至關重要。

問題四

我們是否將評估廠商和合作夥伴的加密敏捷性，作為採購和風險審查程序的一部分？

廠商缺乏後量子就緒程度藍圖，可能會成為薄弱環節。將 PQC 調整納入盡職調查，有助於減少下游風險，並確保長期復原能力。

問題五

我們是否制定有包含治理、自動化和高階主管可見度的分階段、以風險為基礎的遷移策略？

後量子遷移是一個複雜的多年過程。制定包含問責制、自動化部署和即時進度指標的藍圖，對於確保發展勢頭和董事會層級信心至關重要。

高階主管觀點

消除密碼編譯困惑

Wesley Evans
Cloudflare 資深產品經理

組織面臨著加密複雜性激增的問題。過去，我們擁有一些明確定義的標準，而現在，我們擁有一個由演算法和部署模型組成的碎片化生態系統。這種快速演進，加上採用量子安全加密的監管和營運壓力越來越大，在企業層級造成了混亂。

領導者瞭解到要具備加密敏捷性，並為量子復原能力做好準備，但大多數人都不清楚在何處，以及如何使用加密技術。若沒有可見度，規劃就會變成猜測工作。預算停滯不前。擁有權不清晰。這很容易讓高階主管降低行動的優先順序，即使充分瞭解風險亦會如此。

常見缺陷

一個主要的盲點是假設組織尚未遭到入侵。「先竊取、後解密」攻擊切實存在且活躍，尤其是對於具有長期價值的資料，例如，健康記錄、智慧財產權和國家安全資訊。如果您的資料屬於這些類別，可能已經在等待解密能力的威脅執行者手中。

另一個誤解是，量子風險之前會有一個明確的里程碑，就像 Shor 演算法的公開突破。但攻擊者不需要即時結果。

如果破解金鑰需要數週或數月的時間而回報顯著，他們就會進行這項投資。這種感知的延遲會導致一種危險的自滿。

未來方向

兩種轉變正在快速到來。首先，量子糾錯的進步將使量子解密的威脅變得真實，而不是理論。這將增加來自監管機構、董事會和公眾的壓力。其次，組織將開始推出加密敏捷性系統。這意味著最終需要評估加密技術的所在位置、使用方式及擁有者。

這並非易事。大多數團隊對待這個問題，就像早該去看加密牙醫一樣 — 預期會有不適、成本和意外。但等待只會讓情況變得更糟。現在的當務之急不是一蹴而就，而是構建可見度、指派責任，並開始升級路徑。那些盡早行動的組織，將最有能力在後量子轉變成為危機之前進行管理。

「量子糾錯的進步將使**量子解密的威脅**變得真實，而不是理論。」

5

扭轉局勢：治理、地緣政治和道德

扭轉局勢：治理、地緣政治和道德

隨著全球權力的動態變化，網路安全、地緣政治和道德的交集正在重新定義領導層的責任。如今，網路攻擊成為地緣政治影響工具，監管機構追究高階主管個人責任，而 AI 引發的道德困境對傳統監督提出挑戰。

隨著 SEC 於 2023 年要求快速披露網路事件等變更，以及有關國家支援的網路行動的廣泛報導，領導者必須將穩健的治理、透明的 AI 道德規範和敏捷的風險管理納入其策略。

安全治理從指引轉向問責

監管機構的監督不斷加強。2023 年，SEC 要求上市公司在四天內披露網路事件，標誌著向強制問責轉變。近 72% 的公司目前其董事會將優先考慮網路安全專業知識，71% 的公司在至少一份董事傳記中提到網路安全專業知識，而 2018 年這一比例僅為 34%[26]。董事會越來越認識到，忽視網路安全可能會導致嚴重的營運、法律和聲譽後果。

地緣政治和網路戰直接影響企業

民族國家執行者和駭客組織越來越多地將網路行動作為策略性武器加以利用。近年來，國家支援的活動以金融、能源和科技產業為目標，擾亂全球供應鏈並影響市場動態。例如，出於政治動機的威脅執行者 LameDuck 在一年內進行了超過 35,000 次已確認的 DDoS 攻擊，導致 Microsoft、OpenAI 和 Scandinavian Airlines 等組織的營運中斷[27]。即使是表面上中立的組織也可能捲入地緣政治衝突。

必須將高階主管視為攻擊面

公司高層領導者面臨直接的網路威脅。備受關注的深度偽造詐騙和高階主管假冒計畫呈指數級增長，據報告，旨在誤導利害關係人的詐騙性音訊和視訊訊息已將若干 CEO 鎖定為目標[28]。

此類事件凸顯了領導層在面對網路風險，以及針對性的聲譽和金融攻擊時有多脆弱。

監管碎片化和供應鏈不確定性正在加劇

如今，全球企業面臨錯綜複雜的網路安全、AI 和資料主權法律。貿易限制和出口控制迫使公司重新評估廠商關係，以及重新設定供應鏈。例如，不斷變更的關稅和歐盟 NIS2 指令擾亂了既有的供應鏈通訊協定，從而增加了合規成本和操作延遲的風險。

AI 道德規範和影子 AI 要求大規模治理

工作場所中生成式 AI 的爆炸式增長超出組織控制。McKinsey 報告稱，65% 的公司目前在至少一項業務功能中使用 GenAI，而在 2023 年僅為三分之一[29]。2024 年 10 月到 2025 年 2 月，Cloudflare 的 AI Gateway 處理了超過 50 億項請求，短短五個月就增長了 60%[30]。採用迅如閃電：2025 年 1 月，DeepSeek AI 在推出其 R1 模型後的九天內，就在 Cloudflare Radar 的 AI 服務清單上位列第三[31]。

這種基層採用助長了影子 AI 的興起，這是員工在未經授權的情況下使用的工具。這些工具帶來了嚴重的風險：資料外洩、違反監管規定，以及將敏感性資訊暴露給公用模型。

若要做出回應，組織必須超越基本的政策聲明。有效的治理需要明確的核准框架、提示日誌記錄、URL 篩选和用量監控。若不積極地強制執行，AI 道德規範和安全仍將是理論上的。

民族國家執行者和駭客組織越來越多地將網路行動作為**策略性武器**加以利用。

高層面臨的問題

應對道德和地緣政治風險

隨著網路威脅變得地緣政治化、AI 道德規範變得越來越複雜，以及監管預期越來越嚴格，高階主管團隊必須超越技術控制。**以下問題可協助領導者評估他們的治理、情報和回應策略是否適合領導層本身就是威脅面一部分的世界。**

問題一

我們是否有明確的董事會層級問責來實現安全性和數位復原能力，以及定義各種角色和設置具備網路素養的領導層？

鑑於監管機構現在要求高階主管個人承擔責任（如 SEC 的快速披露要求所示），確保董事會具備專門的網路專業知識，對於緩解法律和聲譽風險至關重要。

問題二

我們是否在監控地緣政治變化及其對威脅情勢的影響，包括國家支援的網路攻擊和激進活動？

由於近期國家支援的營運中斷了供應鏈，並瞄準市場關鍵部門，因此，擁有地緣政治風險的相關即時情報對於保障全球營運和領導力至關重要。

問題三

我們是否有主動回應計畫來應對以高階主管為目標的攻擊，例如深度偽造詐騙和假冒活動？

隨著領導層面臨 AI 驅動的錯誤資訊和假冒所帶來的風險日益增大，回應策略必須包括有針對性的事件回應通訊協定和持續的聲譽管理措施。

問題四

我們的原則和網路安全控制是否足夠穩健，能夠偵測並管理員工中未經授權的 AI 使用情況？

隨著越來越多的組織利用 GenAI，以及影子 AI 報告的增加，必須進行精細監控和強制執行嚴格的準則，以防止資料外洩並確保法規遵循。

問題五

我們是否將網路安全和 AI 策略與不斷演進的區域性資料主權和道德 AI 法規保持一致，並且是否將這種一致視為一種策略優勢？

不同的監管框架（例如，歐盟的 NIS2 指令和區域資料主權法律）要求安全性原則既敏捷又具有前瞻性。這種一致性既降低了法律風險，又增強了市場信任和競爭定位。

高階主管觀點

多重危機世界中的治理和問責

Ramy Houssaini
Cloudflare 網路解決方案長

組織必須應對地緣政治、經濟和技術風險交織的多危機情勢。SEC 的網路事件披露要求體現了從網路安全指引向高階主管問責的轉變。組織必須提升即時漏洞偵測和回應能力。不合規會面臨嚴厲的處罰，而聲譽受損可能會削弱利害關係人的信任。董事會必須嵌入網路安全專業知識和主動風險管理，才能保持復原能力。

盲點：地緣政治、AI 和供應鏈風險

一個主要盲點是低估地緣政治網路威脅。許多企業假設中立，但國家支援的攻擊對金融、科技和能源業的擾亂日益增加，使供應鏈變得易受攻擊。

另一個被忽視的風險是影子 AI — 在未監督的情況下使用未經授權的 AI 工具。若沒有穩健的監控，敏感性資料可能會暴露，導致監管處罰和競爭劣勢。

此外，第四方和第五方廠商會引入隱藏的漏洞。雖然公司專注於直接供應商，但擴展的廠商生態系統往往缺乏可見度，使其容易受到網路威脅和營運中斷的影響。

未來發展和策略準備

在接下來的 12–18 個月內，組織應預期：

- **監管擴展：**歐盟的 NIS2 指令和類似框架將加強合規性要求。領導者必須建立監管工作小組才能保持領先。
- **AI 治理加速：**隨著影子 AI 的激增，監管機構將實施更嚴格的控制。公司必須強制執行監控和治理架構來緩解風險。
- **以高階主管為目標：**深度偽造詐騙和假冒攻擊將變得越來越複雜，從而增加詐騙和錯誤資訊的風險。組織應部署 AI 驅動的偵測系統並加強高階主管安全培訓。
- **供應鏈復原能力：**網路威脅和地緣政治不穩定將繼續影響供應鏈。企業必須加強風險評估、強制執行安全義務並改善廠商監控。

為了在這個多危機時代取得成功，領導者必須將網路安全整合至治理中、評估地緣政治風險、強制執行 AI 監督，並建立彈性的供應鏈。敏捷性和卓越的風險管理，對於應對不斷演進的法規和確保長期穩定性至關重要。

「董事會必須**嵌入網路安全專業知識和主動風險管理**，才能保持復原能力。」

結論

公司高層決策：建立規模化復原能力

網路安全的性質已經發生變化 — 現已觸及企業的每一個角落。2025 年，AI 支援的攻擊、地緣政治風險、監管複雜性，以及供應鏈相互依賴性等問題都將出現，需要協調一致的跨職能回應。保障未來不僅僅是對威脅做出回應；更意味著將復原能力嵌入到組織的營運、創新和發展方式中。這些行動號召旨在讓 CXO 通力協作，將復原能力打造為一種策略能力。

1 將復原能力作為共同的策略性任務

確保公司高層在安全狀態、資源配置和應急規劃方面團結一致，以建立跨職能部門的網路安全擁有權。復原能力並非一個團隊的工作，而是一種必須跨職能和跨地區擴展的企業能力。

2 藉由自動化和整合來確保可擴展性

手動合規性和碎片化防禦無法跟上 AI 帶來的威脅和不斷擴大的監管要求。投資自動化以實現威脅偵測、合規性工作流程和事件回應。整合合規性、風險和安全工具，以消除孤島並改善可見度。

3 重新思考將網路治理視為一種競爭優勢

隨著高階主管責任不斷增加，確保您的董事會和高層具備網路素養領導力並規範數位風險監督角色。將網路風險嵌入到企業風險框架中，並將監管一致性視為競爭優勢。

4 從現在開始與時俱進，而不是以後

立即開始您的後量子 (PQC) 加密遷移和 AI 治理準備工作。領導者一直等待，會發現自己很容易受到「先竊取、後解密」的威脅或不受控制的 AI 蔓延。可見度、廠商加密敏捷性和分階段遷移策略是關鍵。

5 失敗測試 — 大規模

復原能力並不是要避免失敗；而是要透過失敗來運作。模擬真實世界的危機 (從超流量 DDoS 到內部人員濫用或以高階主管為目標的攻擊)，並對偵測、遏制和復原能力進行壓力測試。將合規性、通訊和供應鏈因素納入您的情境。

6 在進攻和防禦中整合 AI

AI不應再僅視為一種工具；而是公司高層的一項策略性能力，從而推動整個企業的敏捷性、復原能力和創新。透過充分利用 AI 支援的深入解析，組織可快速適應市場變化、預測風險，以及即時最佳化決策。

AI 藉由自動化威脅偵測、精簡危機回應和加強網路安全狀態，來應對不斷變化的風險，從而增強復原能力。此外，它還透過發現新的營收來源、加速研發，以及大規模提供個人化客戶體驗來推動創新。隨著 AI 深度整合至核心業務職能，它將組織轉變為適應性更強、面向未來的企業，讓領導者能夠自信應對複雜性。

這些行動號召旨在讓 CXO **通力協作，將復原能力打造為一種策略能力。**

保障未來不僅僅是對威脅做出回應；更意味著**將復原能力嵌入到組織的營運、創新和發展方式中。**

Cloudflare 的復原能力：為實現更具擴展性的未來奠定基礎

CLOUDFLARE 的復原能力

與眾不同的可程式設計單一網路

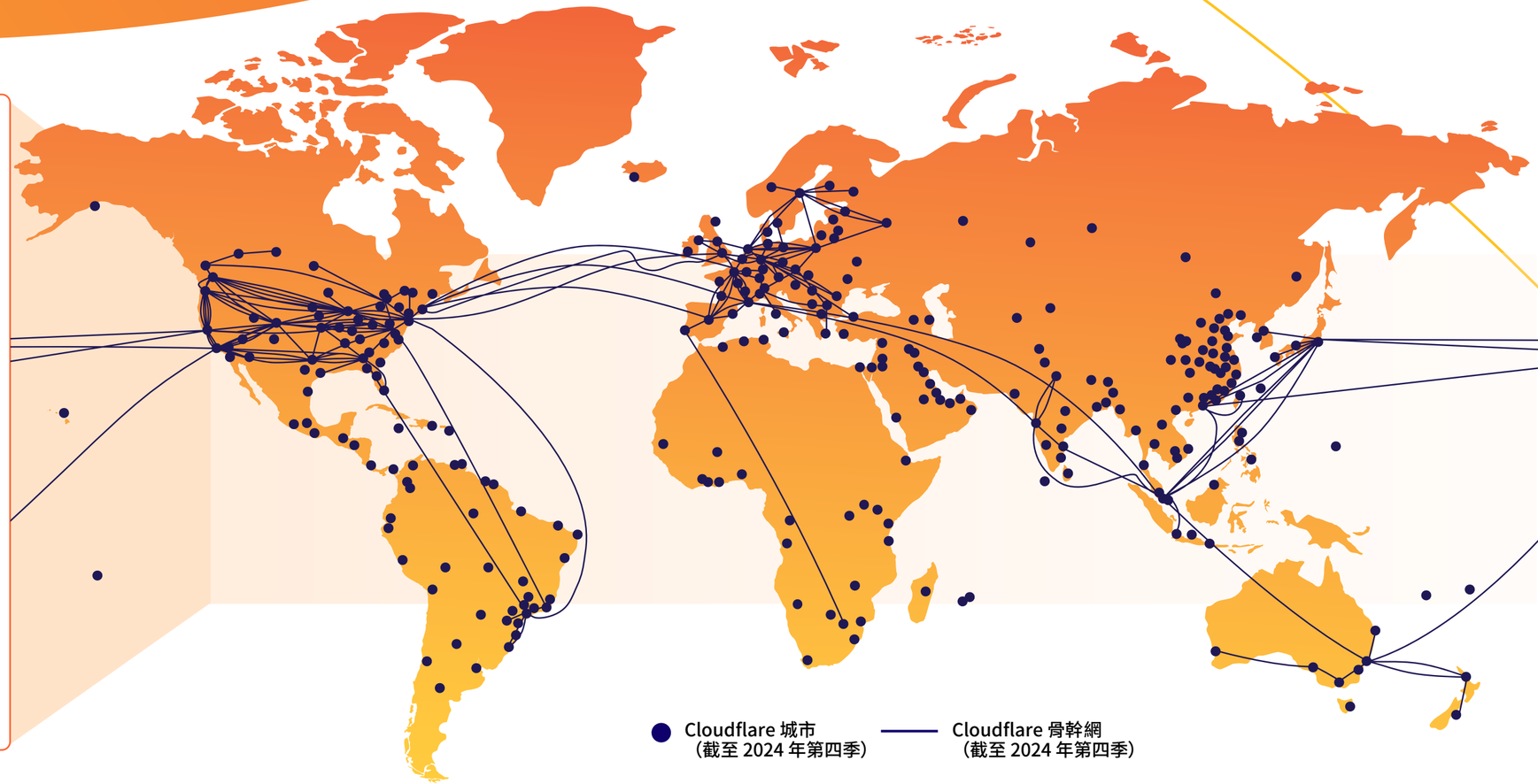
335+ 座城市
遍佈超過 125 個國家/地區，包括中國大陸

↳ **以及 190+ 座城市**
由 GPU 支援進行 AI 推斷

~50 毫秒
連線至約 95% 的全球網際網路連線人口

~13,000 個網路
直連連線至 Cloudflare，包括 ISP、雲端提供者和大型企業

348 Tbps
網路容量，並在持續增長中



CLOUDFLARE 的復原能力

Cloudflare Workers

開發人員構建和擴展 AI 推斷和代理的最佳平台

成本與可擴展性

縱向擴展與縮減至零

在 GPU 上執行 AI 模型，而無需提前數月為尖峰期資源付費。只需依您的實際用量付費。

無運算 = 無用量費

以運算為基礎的定價意味著，若您的功能處於閒置狀態並等待 I/O，您無需支付費用。（應用程式在 I/O 上等待的時間比實際使用 CPU 的時間多 **10 倍**。）

效能

在全球各區域部署

全球約 95% 的網際網路連線人口可在 50 毫秒內執行程式碼。

在一處進行協調和執行

Workers 能夠與 API、LLM 以及外部或內部服務互動，在其最高效的任意位置執行。

開發人員體驗

整合您所需的所有產品

在一個平台存取推斷、狀態管理、UI 部署或工作流程。

幾秒鐘內即可將創意轉化為生產

輕鬆的開發體驗，包括本機開發和快速部署。

節省時間

無需調校。自動放置以獲得最佳效能。

您只管撰寫程式碼，其餘事情交給我們。

CLOUDFLARE 的復原能力

統一的安全平台。網路到雲端。應用程式到 AI。

讓組織能夠：

- 重新獲得營運控制
- 改善網路安全狀態
- 加速廠商整合
- 增強使用者體驗和生產力
- 實現資料治理與合規性

CLOUDFLARE 的復原能力

Cloudflare 面向未來而建置

統一的組合式平台

統一的安全性
適用於面向外部的系統和內部資源

任意連線
適用於使用者、應用程式、分支機構、資料中心和雲端

靈活性
自訂具有完整堆疊開發人員工具的平台

統一的可程式設計的網路

更有效
簡化連線和原則管理

更高效
確保隨時隨地提供快速、可靠和一致的使用者體驗

更敏捷
透過快速創新來滿足不斷變化的安全性要求

CLOUDFLARE 的復原能力

在全球首個分散式無伺服器 AI 推斷平台 Workers AI 上執行推斷任務

全球
各區域部署

335+ 座城市
遍佈超過 125 個國家/地區，包括中國大陸

全球約 95% 的網際網路連線人口可在 50 毫秒內執行程式碼

190+ 座城市
使用 GPU

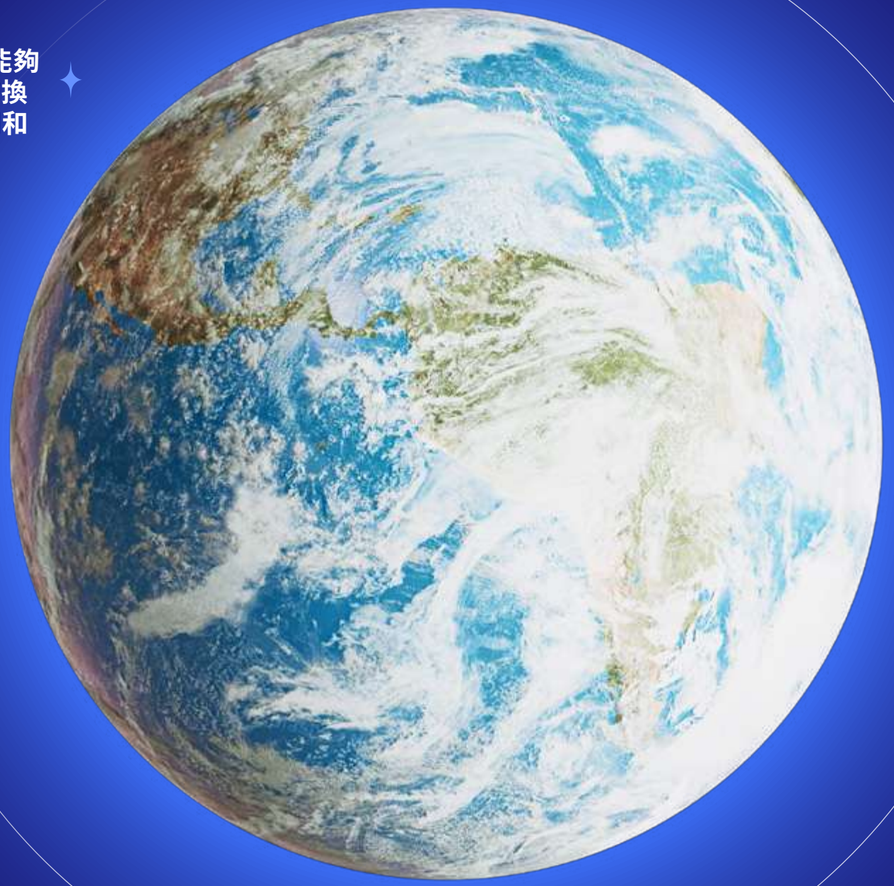
越來越多的城市將採用由 GPU 提供支援的 AI 推斷

CLOUDFLARE 的復原能力

為開放的網際網路而戰

網際網路是一個奇蹟。憑藉採用共同標準的不同網路連線，我們能夠以一種彈性、可互通且任何人都能便捷存取的方式，在世界各地交換資料。如今，我們依賴網際網路來實現經濟增長和創新、資訊取用和言論自由，以及法治和民主原則。

能夠成為全球支援網際網路社群的一員，Cloudflare 備感自豪。



- 倡導網路中立性
- 監控未開放網際網路的場所
- 保護人權與民主機構
- 部署標準以改善資料流的隱私權和安全性
- 參與網際網路標準制定
- 支援多利害關係人網際網路治理

CLOUDFLARE

2025 年 Cloudflare 趨勢觀察報告

瞭解更多

大規模復原能力

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

REV:BDES-6966.2025APR24

章節附註

本報告中的調查結果主要基於 2024 年 1 月 2 日至 2024 年 12 月 31 日期間，在 Cloudflare 全球網路中觀察到的彙總流量模式。

1. https://www.darktrace.com/blog/survey-findings-ai-cyber-threats-are-a-reality-the-people-are-acting-now/
2. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
3. Cloudflare Radar 分析，2024 年
4. https://www.cnbc.com/2025/02/24/chegg-sues-google-for-hurting-traffic-as-it-considers-alternatives.html; https://www.theguardian.com/gnm-press-office/2025/feb/25/make-it-fair
5. Cloudflare Radar 分析，2024 年
6. https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf
7. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
8. https://www.verizon.com/business/resources/T1e3/reports/2024-dbir-data-breach-investigations-report.pdf
9. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/bots
10. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/; https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11. Cloudflare Radar 分析，2024 年
12. Cloudflare Radar 分析，2024 年
13. https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/
14. https://therecord.media/advance-auto-parts-data-breach-2million
15. Cloudflare Radar 分析，2024 年 10 月 12 日至 2024 年 12 月 31 日
16. Cloudflare Radar 分析，2024 年 10 月 12 日至 2024 年 12 月 31 日。https://radar.cloudflare.com/security/application-layer
17. Cloudflare Radar 分析，2024 年。https://blog.cloudflare.com/tag/ddos-reports/
18. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/reports/ddos-2024-q4
19. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
20. https://www.verizon.com/business/resources/Tdd6/reports/2024-dbir-data-breach-investigations-report.pdf
21. Cloudflare Radar 分析，2024 年
22. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf
23. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-survey-findings-on-esg-disclosure-and-preparedness.pdf
24. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
25. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/adoption-and-usage
26. https://www.ey.com/en_us/board-matters/cyber-disclosure-trends
27. https://www.cloudflare.com/threat-intelligence/research/report/inside-lameduck-analyzing-anonymous-sudans-threat-operations/
28. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
29. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024
30. Cloudflare Radar 分析，2024 年 10 月至 2025 年 2 月
31. Cloudflare Radar 分析，2025 年 1 月。https://radar.cloudflare.com/ai-insights