CLOUDFLARE

AI 時代的五大網路安全趨勢

5

龔念弘 Neo Kung, Cloudflare 大中華區資深解決方案顧問

CLOUDFLARE

全世界有超過 20% 的流量經過 Cloudflare
Cloudflare 看到那五大趨勢？

1

對抗 AI

在對抗 AI 的時代
保護企業

2

超越邊界

Zero Trust、
身分和新的
安全前沿

3

超大體量短促的 DDoS

在基礎架構、
生態系統和監督
中擴展保護

4

又要快又要安全

太慢用戶就跑了
效能與安全之間的
取捨還是問題

5

治理與合規

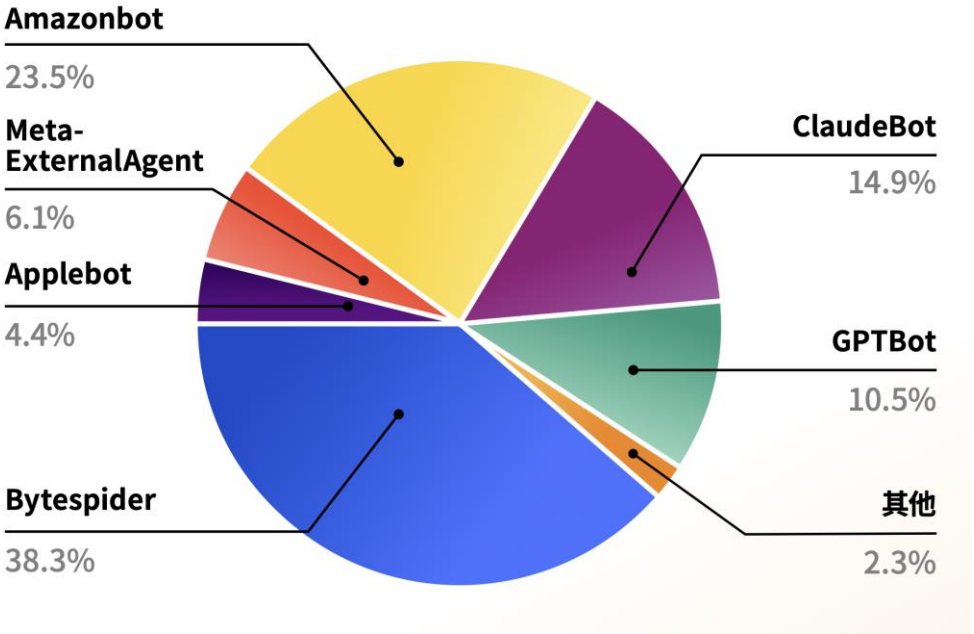
AI、金融與資安
法規加速落地，
企業需要能即時
展示控制與
稽核的能力

1

對抗 AI

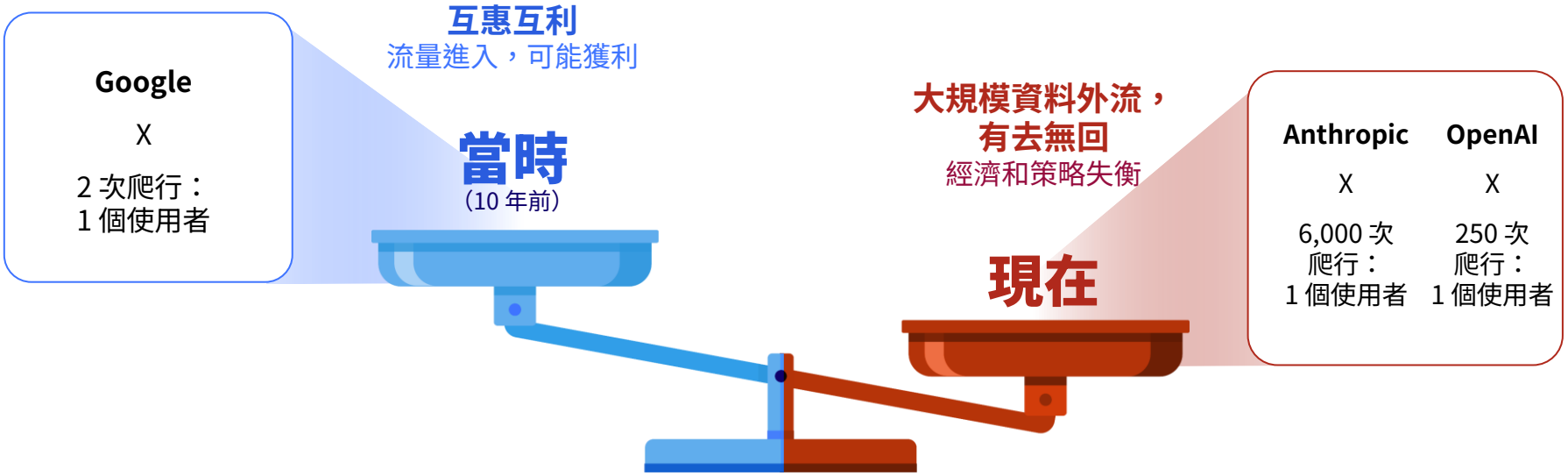
在對抗 AI 的時代保護企業

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



CLOUDFLARE

過去是互惠交換，現在 AI 爬蟲卻是大量索取、回流極少，成本都留在網站。



CLOUDFLARE

AI 驅動的資安現況: AI 索取多、攻擊快，防守必須自動化

1 AI 爬蟲大量索取卻少回流

AI 平台透過爬蟲大規模抓取資料，卻幾乎沒有帶回流量，網站承受基礎設施成本卻得不到效益。

28% 應用程式流量來自機器人

2% 其中，AI 爬蟲佔據前面 28% 的 2%

2 攻擊速度加快、傳統防禦失效

攻擊者用 AI 自動化滲透與逃避偵測，速度比人還快，傳統手動安全措施跟不上。

74% IT 安全專業人員表示 AI 驅動的威脅已嚴重影響組織

快 AI 驅動的工具能協助快速製作釣魚郵件、甚至「黑暗聊天機器人」可自動寫出惡意程式

3 防守也必須 AI 自動化

靠人力或傳統規則防守已不可能，必須用 AI 偵測、AI 防護來追趕 AI 攻擊。

93% AI 機器人流量沒有帶來任何實際價值

來源：DarkTrace State of AI in Cybersecurity（網路安全領域 AI 現狀）| Experian ‘Synthetic fraud’ reaches record levels（合成詐欺達到歷史新高水準）| National CIO Review Insider Threat Report（內部人員威脅報告）

CLOUDFLARE

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 1

我們有沒有用 AI 來看清楚所有安全狀況？

是不是能統一記錄、分析、警示，知道問題在哪裡？

問題 2

我們能不能靠 AI 即時抓到威脅並自動處理？

不是等到事後，而是發生時馬上應對。

問題 3

我們擋得住 AI 幫助的釣魚、深偽和惡意程式嗎？

攻擊手法在進化，防護也要跟著升級。

問題 4

我們的敏感資料能防住 AI 爬蟲和自動竊取嗎？

有沒有機器人管理、API 驗證或數位浮水印來保護？

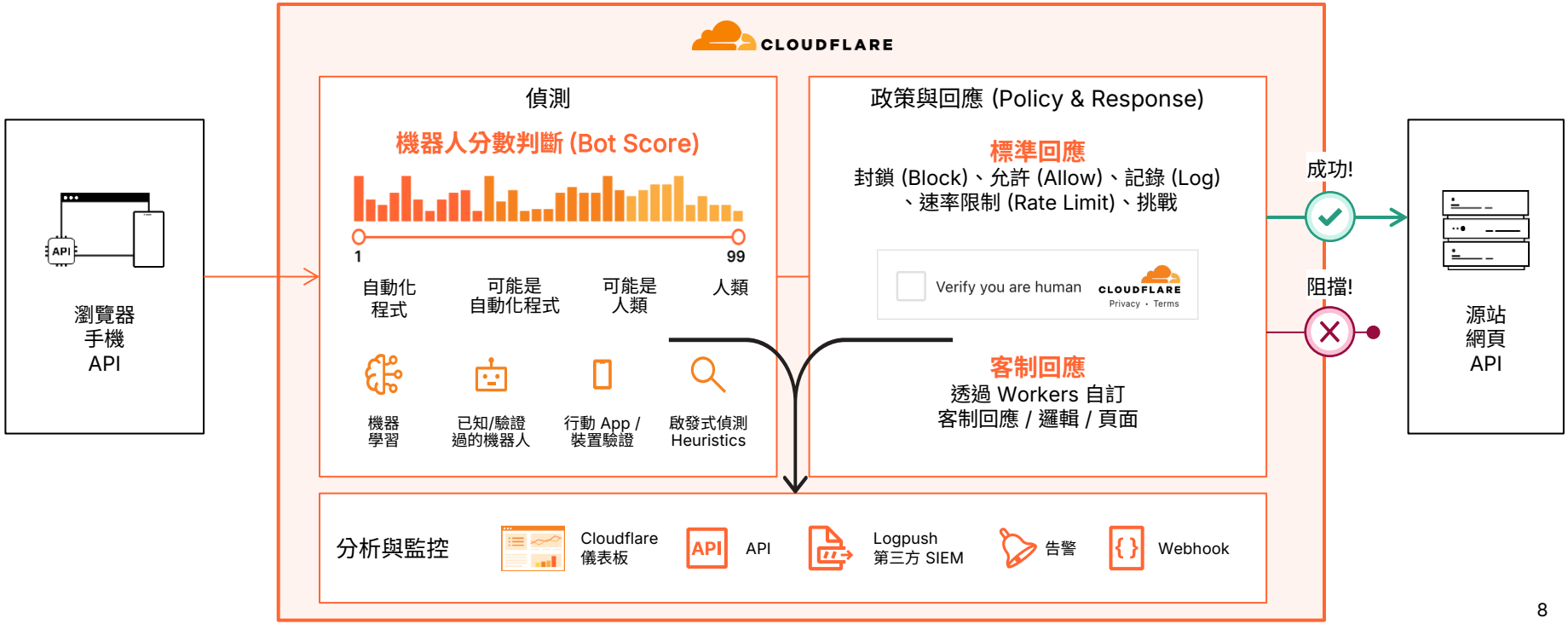
問題 5

我們有沒有用 AI 偵測內部同仁的異常行為？

例如存取模式怪異、權限亂提、資料外流

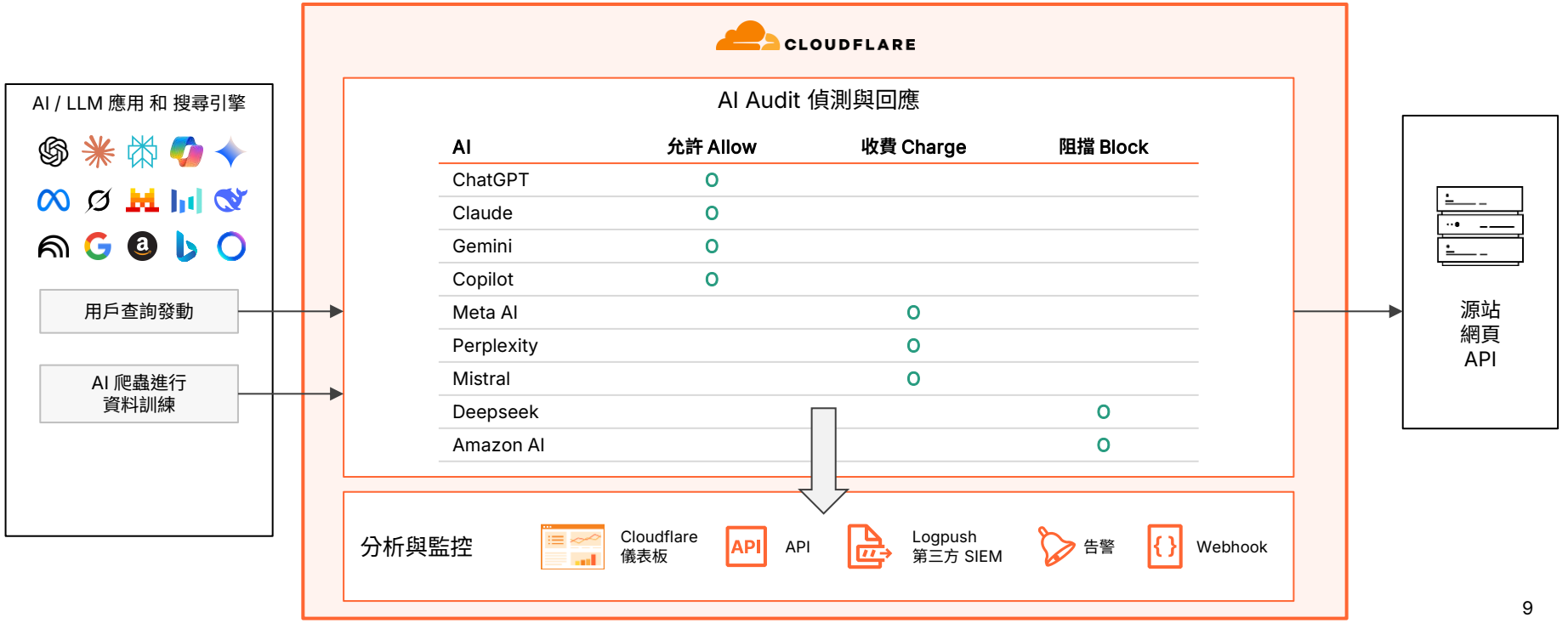
CLOUDFLARE

機器人防堵能辨識出真實用戶 / 機器人，並有效防堵爬蟲、惡意使用，替您節省網路費、維持服務穩定性！



CLOUDFLARE

讓您清楚看到哪些 AI 服務（如 OpenAI, Claude, Perplexity 等）正在存取哪些內容、存取頻率，再決定是否允許或封鎖



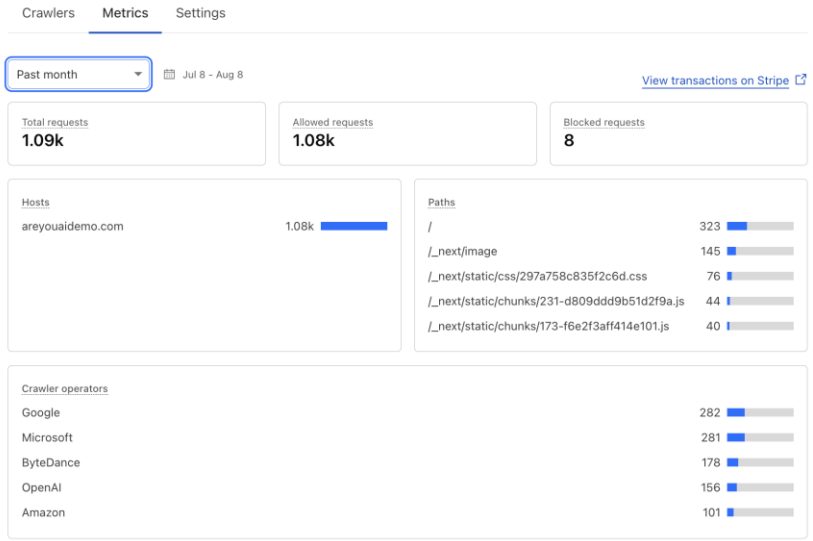
CLOUDFLARE

讓您清楚看到哪些 AI 服務（如 OpenAI, Claude, Perplexity 等）正在存取哪些內容、存取頻率，再決定是否允許或封鎖

一鍵式操作超簡單，**放行**｜**收費**｜**阻擋**

Crawler	Operator	Category	Allowed requests	Robots.txt violations	Action
Googlebot	Google	Search Engine	282	0	Allow Charge Block
BingBot	Microsoft	Search Engine	281	0	Allow Charge Block
Bytespider	ByteDance	AI Crawler	178	0	Allow Charge Block
Amazonbot	Amazon	AI Crawler	101	0	Allow Charge Block
GPTBot	OpenAI	AI Crawler	75	0	Allow Charge Block
PetalBot	Huawei	AI Crawler	49	0	Allow Charge Block
ChatGPT-User	OpenAI	AI Assistant	43	0	Allow Charge Block
OAI-SearchB...	OpenAI	AI Search	38	0	Allow Charge Block
Meta-Extern...	Meta	AI Crawler	22	0	Allow Charge Block
ClaudeBot	Anthropic	AI Crawler	10	0	Allow Charge Block
Applebot	Apple	AI Search	2	0	Allow Charge Block
Anchor Brow...	Anchor	AI Crawler	0	0	Allow Charge Block

定期追蹤使用狀況，如請求數、放行數、最受歡迎路徑等



CLOUDFLARE

已經有非常多的內容提供商/出版商加入 Cloudflare 的 AI Audit / Pay Per Crawl

ADWEEK
AP
The Atlantic
Atlas Obscura
BuzzFeed
CONDÉ NAST
dcn DIGITAL CONTENT NEXT
Dotdash meredith
Drupal
EVOLVE MEDIA
FORTUNE
GANNETT
(h[s])® HYPERSCIENCE
ib Internet Brands®
linkup
NEWSMEDIA ALLIANCE
O'REILLY®
Pinterest
Quora
ProRata.ai
reddit
sky news
Snopes
sovrn
stackoverflow
Stocktwits
THIRD DOOR MEDIA
TIME
UNIVERSAL MUSIC GROUP
Ziff Davis

Demo 1

AI Audit 如何替您擋住 AI / LLM

- AI Bot 爬蟲分析紀錄與禁止
- AI Audit 的分析儀表板
- Cloudflare Radar 的全球流量機器人分析儀表板

2

超越邊界

Zero Trust、身分識別和新的安全前沿

企業最大的風險：VPN 脆弱、API 看不清、影子 IT 難管、帳密直接被用

1 VPN 已成主要攻擊目標

傳統 VPN 容易被暴力破解與濫用，Zero Trust 已經成為主流替代方案。

74% 的組織表示已計畫或全面用 Zero Trust 架構取代 VPN。

2 未知 API 帶來高風險

很多企業低估自己 API 的數量，導致可見性不足，攻擊面大幅增加。

4 倍 Cloudflare 發現，組織少報了四倍的 API 端點。

3 影子 IT 與未受管控服務讓風險加劇

員工私自使用雲端或 SaaS 平台，會讓公司 IT 安全失去掌控。

38% 的員工曾在 AI 平台或雲端服務分享過公司敏感資料。

4 攻擊者不是「闖入」而是「直接登入」

攻擊者透過外洩帳密，直接登入比入侵更快更隱蔽。

22% 的資料外洩事件，起點是帳密被竊用。

來源：Cloudflare Zero Trust 員工調查問卷，2024 年 5 月 | 2025 年 Cloudflare 趨勢觀察報告 | CybSafe，The Annual Cybersecurity Attitudes and Behaviors Report（年度網路安全態度與行為研究報告）| Verizon DBIR，2025 年

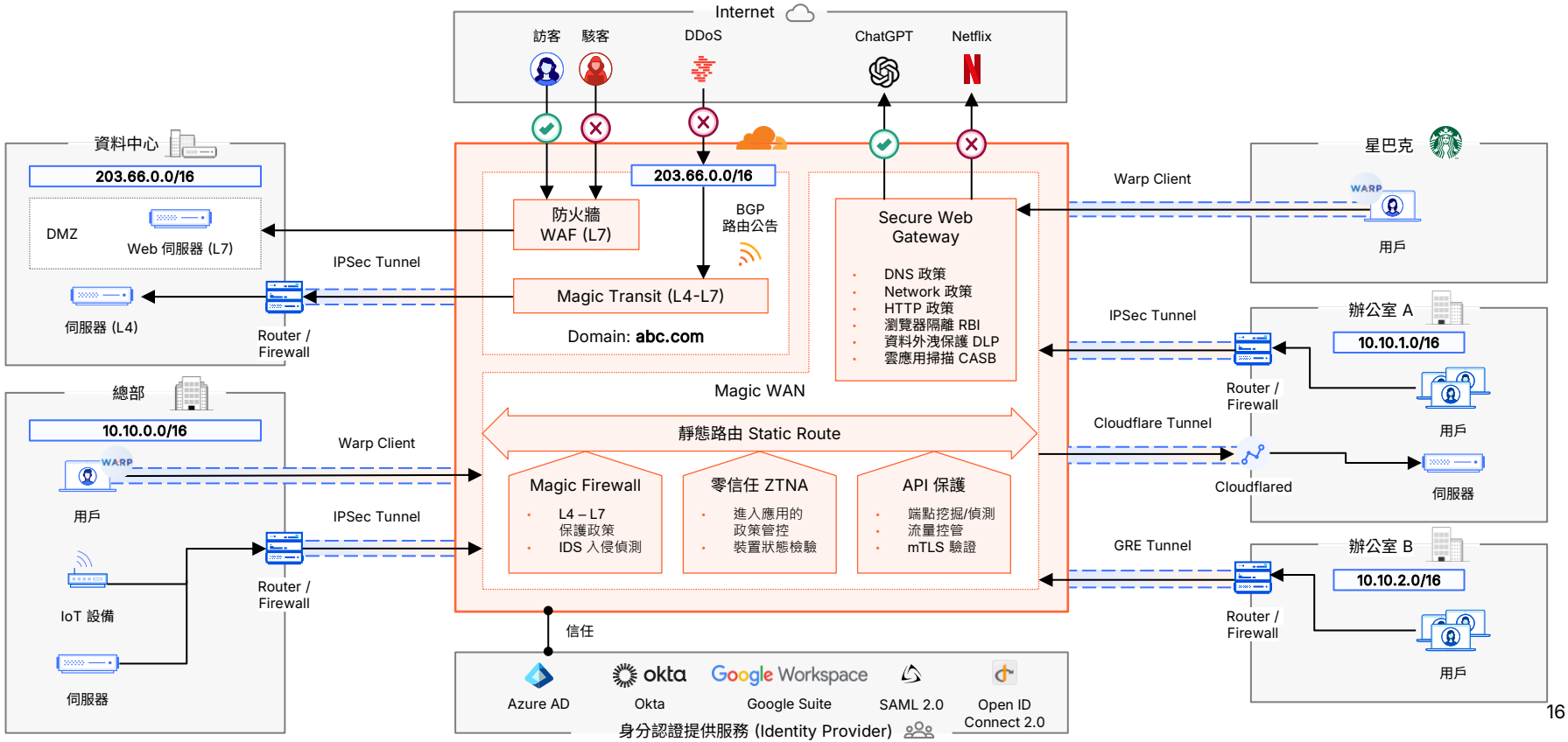
CLOUDFLARE

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 1	問題 2	問題 3	問題 4	問題 5
我們的雲端、SaaS 和 API 有沒有真的做到 Zero Trust？	**我們知道員工用了多少影子 IT 和未受管的雲端服務嗎？**	**我們的 API 有沒有好好保護，避免被濫用或外洩？**	**我們是不是還在靠密碼撐安全？**	**我們能不能即時分辨並攔截自動化攻擊？**
有沒有落實最小權限、全面驗證？	有沒有掌握未經批准的 SaaS 使用？	有沒有防止未授權的存取和資料外流？	有沒有做到無密碼驗證或更強的驗證方式？	AI 機器人 vs. 人類，有沒有辦法快速偵測與防禦？

CLOUDFLARE

Cloudflare SASE 架構



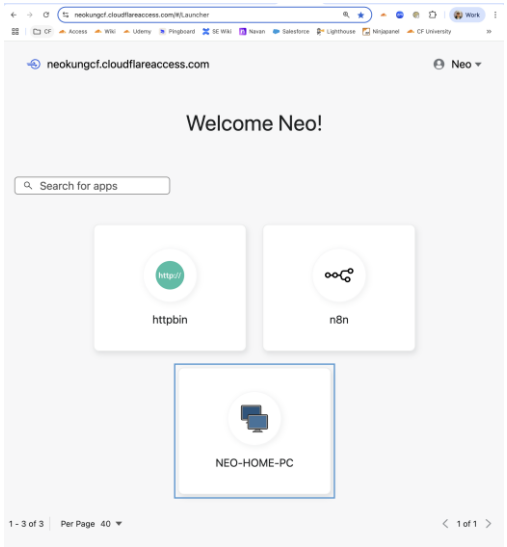
用戶登入的流程

用戶透過 Warp 連上

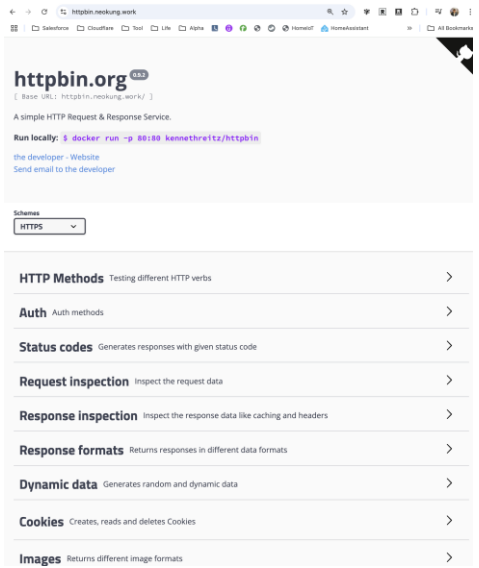
透過 Azure AD 結合 MFA 進行驗證

- 透過 Warp 收集裝置狀態

進入 App Launcher



進入應用



CLOUDFLARE

自動發掘並盤點 API 端點；透過 mTLS 互驗憑證攔截未授權請求；驗證資料格式與允許方法，確保 API 呼叫安全且符合業務邏輯。

自動挖掘 API 端點；盤點不費力

Identify, analyze, and protect your APIs by enabling Cloudflare's API security, management, and monitoring services.

Your API Shield preview

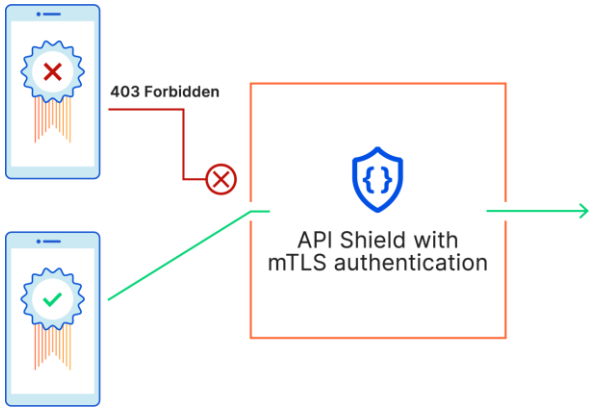
Total requests	API requests	Discovered endpoints
7.62M	1.2M 15%	140

In the past 24 hours, API requests were **15% of your total requests**. Preview API Shield to **140 discovered endpoints**, access API analytics like error rates, and validate traffic agains

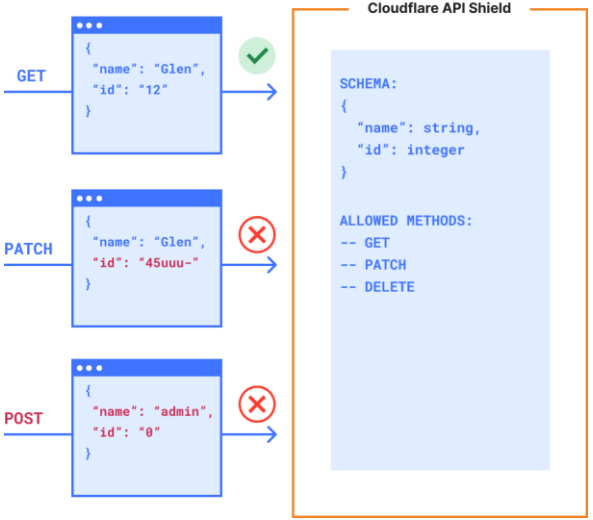
Top 10 discovered endpoints

Method	Endpoint	Hostname	Requests
GET	/secret-endpoint/{var1}/login	api.host.com	845k
GET	/secret-endpoint/2	api.host.com	300k
DELETE	/secret-endpoint/2	api.host.com	125k
GET	/secret-longer-...point/value	api.host.com	118k
GET	/secret-endpoint/2	longer.api.ho...me.org	60k
GET	/secret-endpoint/2	api.host.com	60k
GET	/secret-endpoint/2	api.host.com	60k
UPDATE	/secret-endpoint/2	api.host.com	60k
GET	/secret-endpoint/2	api.host.com	60k
GET	/secret-endpoint/2	api.host.com	60k

前端後端互驗憑證 (mTLS)，確保安全



驗證請求的資料格式，業務邏輯正確有保障



3

超大體量/短促的 DDoS

在基礎架構、生態系統和監督中擴展保護

DDoS 攻擊更猛、更快、更自動化

1 攻擊量大幅上升

DDoS 已成為常態化威脅，
攻擊次數持續飆升。

2,090 萬次
攻擊在 2024 被 Cloudflare 封鎖 ，

50%
更多的攻擊，
比起 2023 年

2 攻擊規模更極端

超流量攻擊已經突破歷史新高，
速度和強度都刷新紀錄。

1,885%
2024 年 Q4，
超過 1 Tbps 的攻擊
數量季增

175%
每秒超過 1 億封包
(pps) 的攻擊增加

3 攻擊更自動化

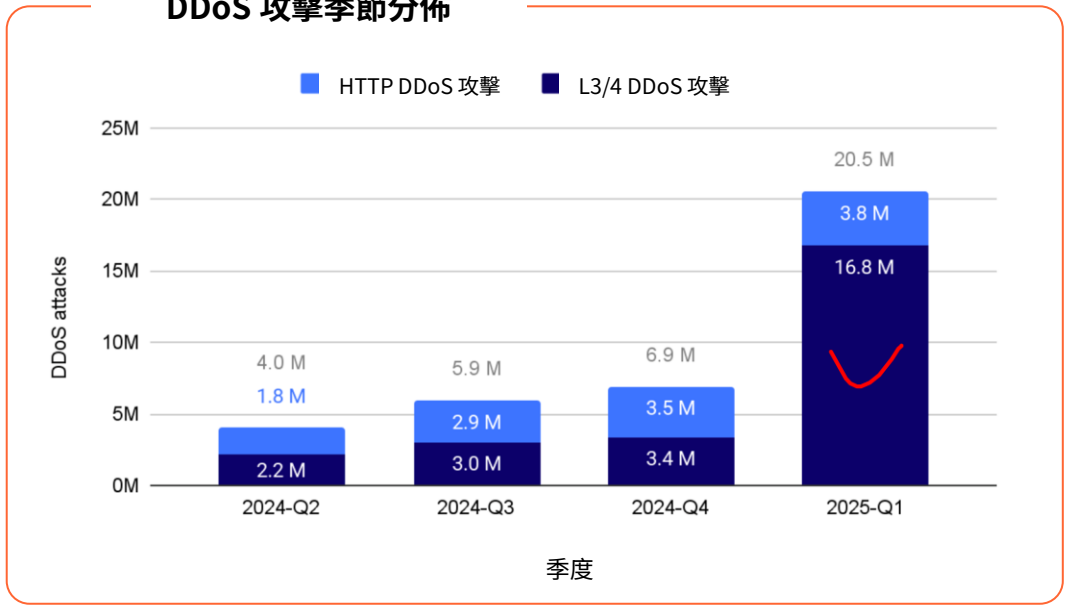
攻擊者運用殭屍網路、IoT 裝置
和 AI 工具自動化攻擊，
速度快於傳統防護。

10 億 pps
的攻擊規模佔據至少 16%
靠人工幾乎不可能
即時防禦。

來源：2025 年 Cloudflare 趨勢觀察 | DHS Harmonization of Cyber Incident Reporting to the Federal Government（聯邦政府網路事件報告標準化方案）| Deloitte Sustainability Action Report（永續發展行動報告）

2025 攻擊潮：更大、更短、更難防

- **2025 年第一季的攻擊數為 2050 萬**，幾乎與 2024 年全年持平（總數為 2090 萬）
- 2025 年第一季**超過 700 起超流量攻擊**
- 2025 年第二季**創紀錄的 6.5 Tbps 攻擊**，持續僅 40 秒
- **全部自動偵測和緩解**



CLOUDFLARE

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 1

我們的系統能撐住大規模 DDoS 嗎？

面對數 TB 級別攻擊，服務還能正常跑嗎？

問題 2

能即時掌握第三方服務的健康狀況嗎？

出問題時能馬上知道是哪個供應商拖慢了？

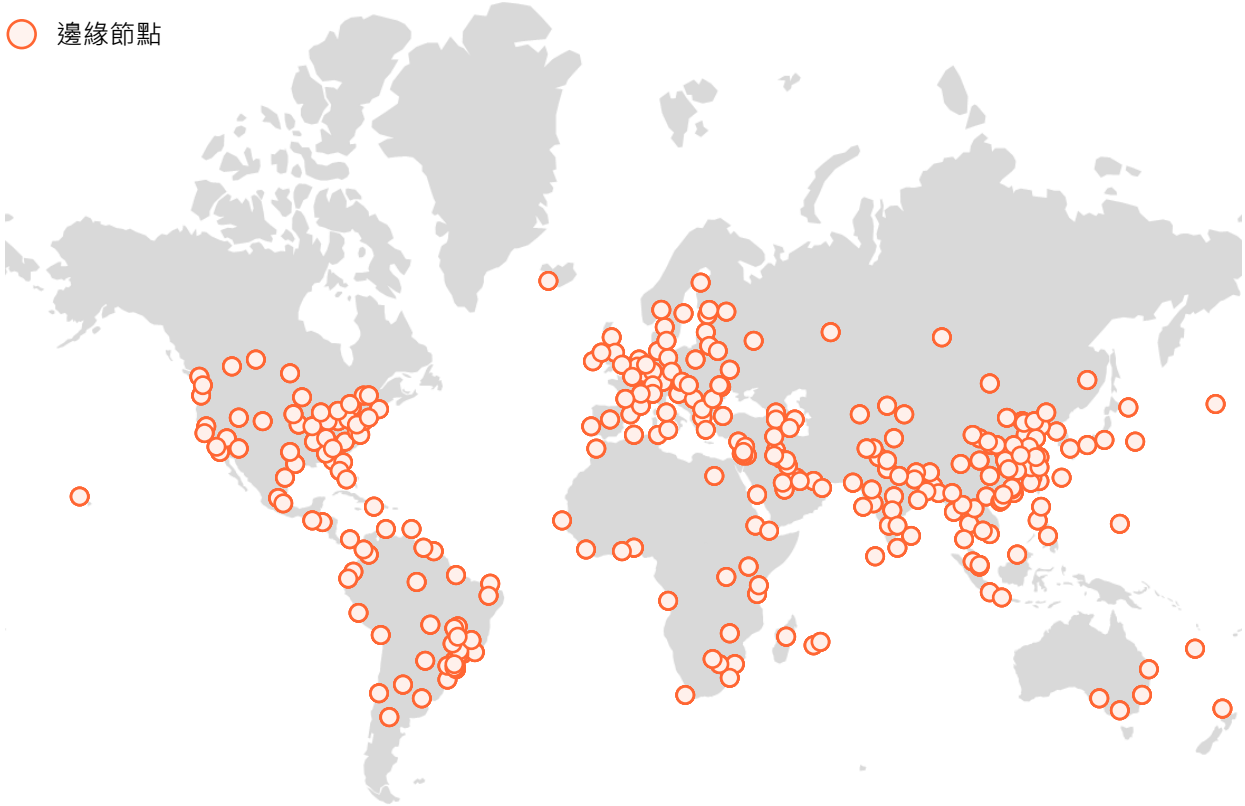
問題 3

合規和安全是否已自動化並整合？

還在分散手動處理，還是能自動化、集中管理？

CLOUDFLARE

全球 335+ 個城市有超過 490 個 PoP（邊緣節點）



每日阻擋超過
2,270 億次網路威脅

網路總容量達
388 Tbps 且持續成長

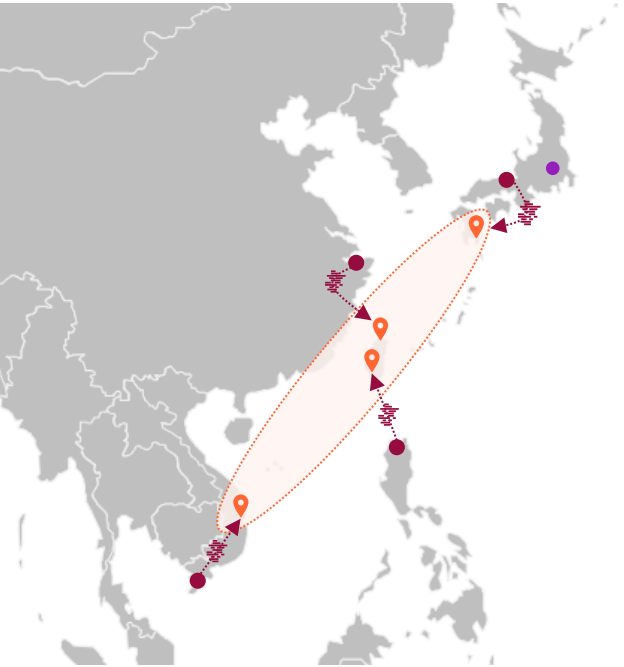
約 **20%** 的網站部署
在 Cloudflare 後面

125+ 個國家擁有
335+ 座城市的節點
包含**台北、高雄、中國**

CLOUDFLARE

DDoS **防禦，**Cloudflare **可以說是市場上佼佼者!**

Cloudflare – **基於 Anycast 自動分流，每個節點都能抵禦 DDoS**



網路總容量達

388 Tbps

且持續成長

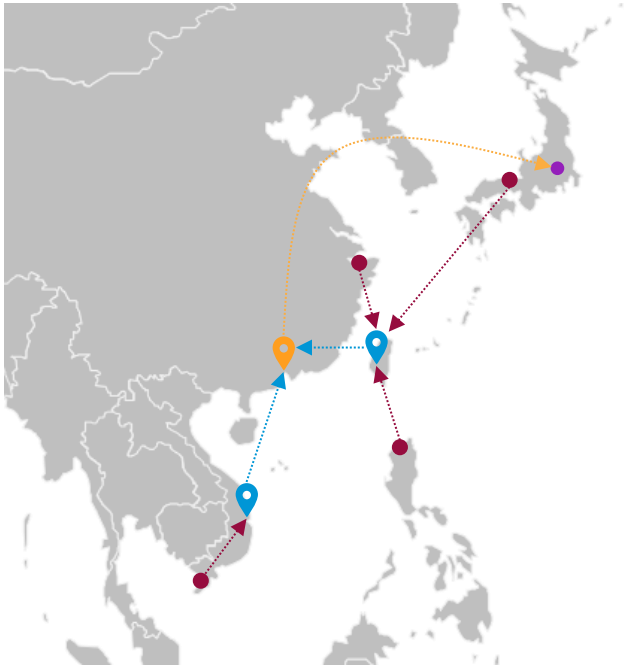
Cloudflare Anycast 網絡

Cloudflare POP

DDoS 攻擊

源站

他牌 DDoS 清洗 - **一般節點 Unicast，清洗中心 Anycast**



POP

清洗中心

DDoS 攻擊

流量轉發

乾淨流量轉發

源站

4

又要快
又要安全

太慢用戶就跑了，效能與安全之間的取捨還是問題

CLOUDFLARE

速度優化三關鍵：砍 JS、上 H3、用好 bfcache

1 頁面越來越肥，JS 是主因

頁面體積逐年上升，JS 檔數與大小是主要拖慢速度的原因。

22 - 24 個 JS 檔案在一個頁面

2 HTTP/3 使用率快速成長

H3 已成主流傳輸協定，支援度逼近三成，流量已突破兩成。

20.5% 2024 全球流量 HTTP 3 佔比

3 bfcache 沒被好好利用

回上一頁原本能「瞬回」，但不少網站因 no-store 阻擋快取。

21% 網站用了 no-store，所以 bfcache 沒被啟用。

CLOUDFLARE

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 1

我們的數位服務速度，是否已影響用戶體驗與留存？

客戶是不是因為速度慢，直接流失到競爭對手？

問題 2

我們有投資在未來的網路效能基礎上嗎？

HTTP/3、全球加速等新技術，是否已經納入規劃？

問題 3

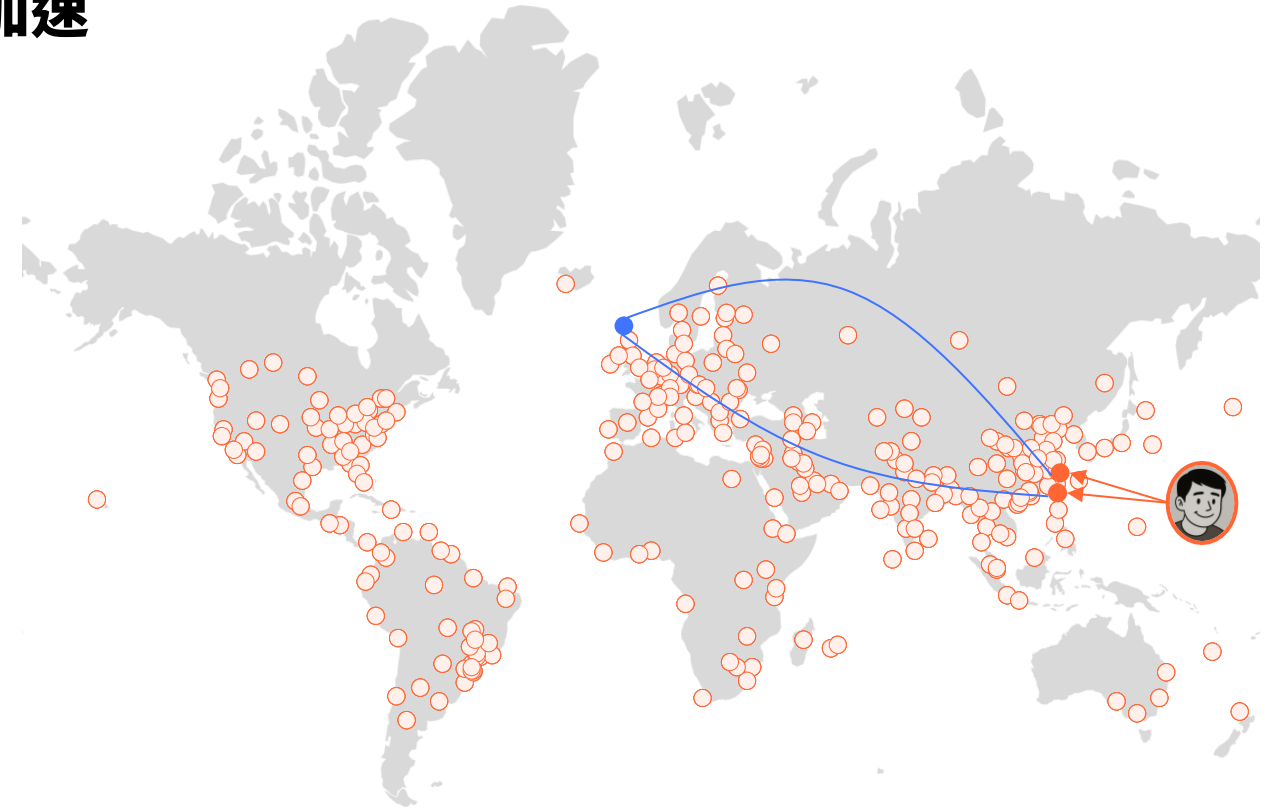
我們是否善用現有瀏覽器與平台優化機制？

是不是還有「零成本」的效能紅利沒有被啟用？

CLOUDFLARE

全球 335+ 個城市有超過 490 個 PoP（邊緣節點）將靜態資源快取實現加速

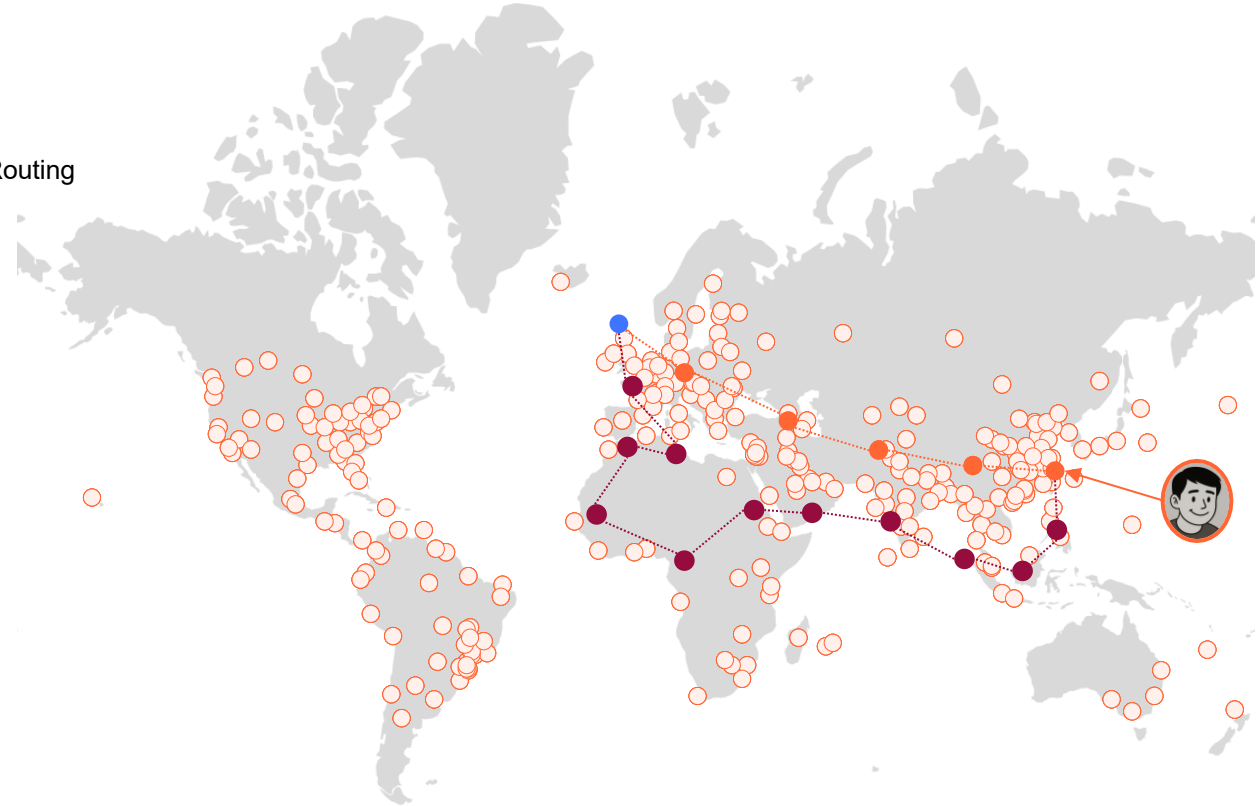
- 邊緣節點
- 源站
- 用戶拿到靜態資源的節點



CLOUDFLARE

根據實際網絡情況選擇最優的路由調度路徑

- 邊緣節點
- 源站
- 利用 Argo Smart Routing 的節點
- 一般 ISP 站點



5

治理與合規

AI、金融與資安法規加速落地，企業需要能即時展示控制與稽核的能力

三大現實：全球風險、合規壓力、AI 衝擊

1 地緣政治與網路戰成常態

地緣衝突與駭客集團讓產業全面受影響，攻擊規模空前。

35,000 起 DDoS 攻擊來自單一駭客組織

2 合規要求推向資料 & AI 推論在地化

自 GDPR（2018 年）生效以來，有至少 30 個國家制定或修訂了資料保護法，其中許多包含限制個人資料跨境傳輸的條款

13 億美元 2023 年，Meta 因將個人資料從歐盟轉移到美國，且沒有對轉移的資料提供足夠的隱私權保護而被罰款

3 AI 帶來新挑戰與快速變革

AI 風險治理迫在眉睫，生成式 AI 帶來前所未有的速度與壓力。

58% 組織已開始 AI 風險評估

9 天 DeepSeek 躍升第三大 AI 服務

資料來源：EY，Cybersecurity oversight disclosures: what companies shared in 2024（2024 年企業網路安全監督揭露現況報告）| Cloudflare，Inside LameDuck: analyzing Anonymous Sudan’s threat operations（深入剖析 LameDuck：駭客組織 Anonymous Sudan 的威脅行動）| The Guardian，《全球最大廣告公司 CEO 淪為深偽詐騙目標》專題報導 | 2025 年 Cloudflare 趨勢觀察報告

CLOUDFLARE

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 1

我們有沒有隨時關注地緣政治，並調整資安防護？

確保能因應不斷變化的威脅情勢

問題 2

我們的 AI 和資料策略，跟各國新出的法規能否對得上？

因應資料主權、AI 合規要求，避免踩紅線

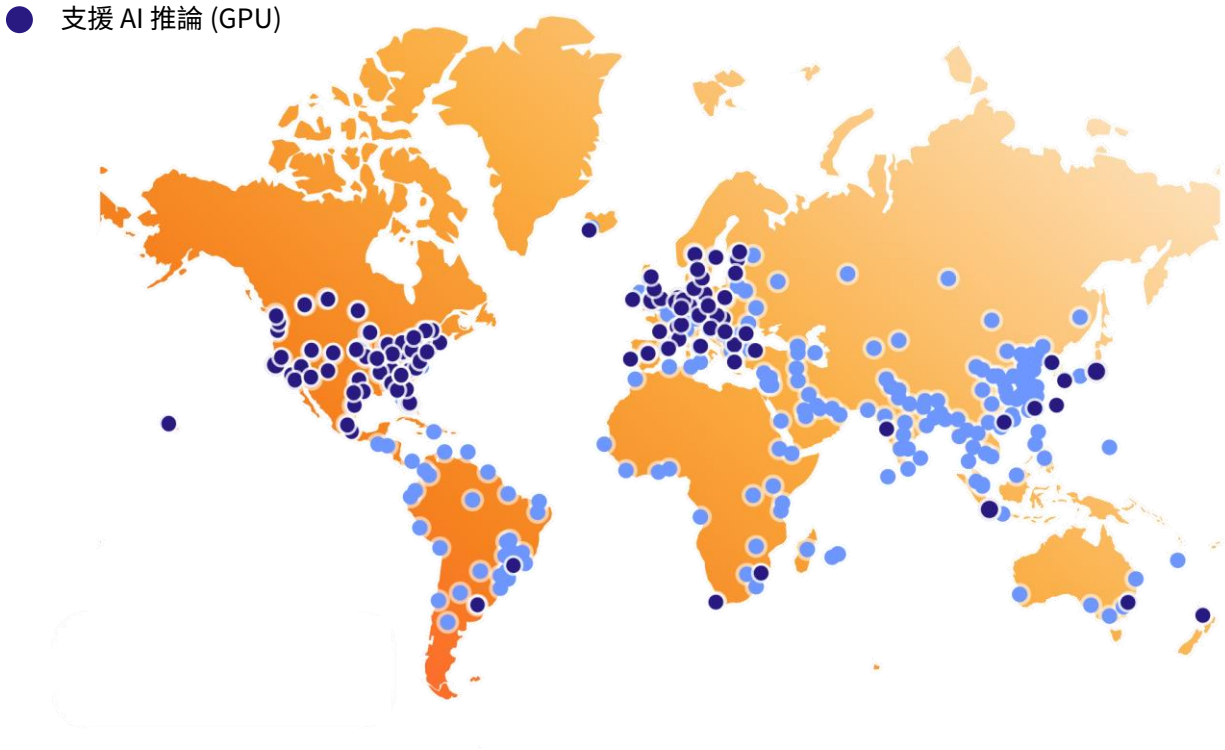
問題 3

我們能不能有效偵測、管控員工私下用的 AI 工具？

避免「影子 AI」帶來資料外洩或風險

CLOUDFLARE

全球超過 490 個 POP 裡面有 190 個以上支援 Workers AI 進行 AI 推論



1

Cloudflare Worker AI 讓您
租用 AI / LLM 服務，按請求數付費！超划算

2

台灣本地 POP 台北跟高雄
都可以做 AI Inference
可以合規，沒問題！

3

全世界 POP 有 190 個以上都支援
離用戶超近速度超快
還有 Cloudflare 老本行 CDN 快取
替您降本增速！用戶體驗超讚

Cloudflare 通過世界各國/各區的主要認證 & 標準，確保合規性

ISO 27001:2022
實施資訊安全管理系統 (ISMS) 和安全風險管理流程認證。

ISO 27701:2019
實施全面的隱私資訊管理系統 (PIMS) 認證。

ISO 27018:2019
延伸 ISMS 以保護在雲端處理的個人資料；隱私認證。

FedRAMP Moderate
美國聯邦風險與授權管理計畫。

PCI DSS 4.0
支付卡產業資料安全標準合規證明。

全球 PRP
透過全球處理者隱私認可（全球 PRP）系統，參與的組織可以證明自己作為資料處理者符合國際認可的資料保護標準。

BSI 認證
Cloudflare 已獲得德國政府聯邦資訊安全辦公室的認可，成為合格的 DDoS 緩解服務提供者。

全球 CBPR
透過全球跨境隱私規則（全球 CBPR）系統，參與的組織可以證明自己作為資料控制者符合國際認可的資料保護標準。

SOC 2 Type II
用於證明已根據 AICPA 信任服務標準實施安全性、機密性和可用性控制的認證。

ENS
西班牙國家安全框架
Esquema Nacional de Seguridad.

IRAP
Cloudflare for Government 資訊安全註冊評估師計畫 - 澳洲。

Cyber Essentials

WCAG 2.1 AA 和第 508 節
根據《無障礙網頁內容指南》(WCAG) 2.1 AA 中的國際標準，以及《復健法》第 508 節所規定之法定標準，Cloudflare 的儀表板完成了自願產品協助工具範本 (VPAT)。

歐盟雲端行為準則
《歐盟雲端行為準則》是官方核准的 GDPR 第 40 條行為準則。

C5:2020
《雲端運算合規性條件目錄》(C5:2020) 是德國政府聯邦資訊安全辦公室 (BSI) 所建立的稽核標準。

Cloudflare 資料本地化套件

Data Localization Suite 是一組產品與功能，讓您可以控制資料被檢查和儲存的位置，協助企業符合各地區資料隱私法規。

Geo Key Manager
（地理金鑰管理）
可控制 TLS 加密私鑰存放在哪個地區。

Regional Services
（區域服務）
可控制流量在哪個地區被解密和檢查。

Customer Metadata Boundary
（客戶中繼資料界線）
可控制有關流量的中繼資料（metadata）如何處理與儲存。

感謝您的時間

希望 Cloudflare 有機會
協助保護、加速您的網路環境!