樂雲智能有限公司

LEYUN INC.

樂雲為Cloudflare合作夥伴


樂雲 LEYUN

02-77220055

service@leyun.cloud

www.leyun.cloud

Line | @leyun

FB | Leyun.Inc

IG | Leyun.Inc

www.leyun.cloud

# 樂雲
LEYUN

資安防禦領導者

# 目錄

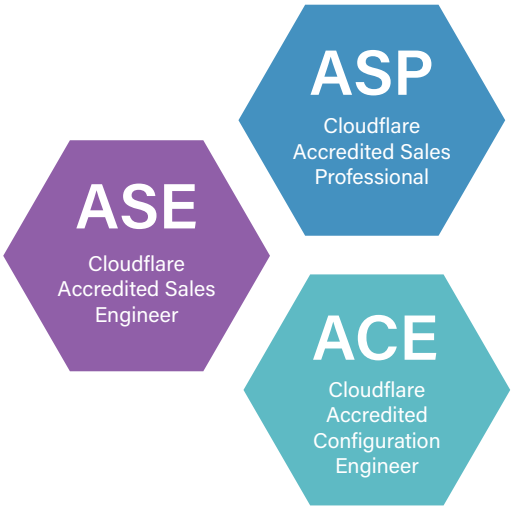
樂雲智能有限公司

LEYUN INC.

樂雲

# 關於樂雲

樂雲智能 Leyun 擁有領先的雲技術服務和豐富的電信及網際網路營運經驗，熟悉各項雲端資安服務領域，透過各項資源的整合提供給客戶更適合的產品介紹，不斷追求更符合顧客所需的雲端資安產品解決方案，致力打造全新的雲服務生態系。用最專業的技術服務，站在客戶角度出發給予最佳產品解決方案。




## 樂雲提供多項雲端產品解決方案

aws

Google Cloud

樂直播 LE STREAM

SECTIGO

LEYUN GLOBAL SERVER

樂雲簡訊 LEYUN

樂雲服務

# Cloudflare 競爭優勢

吸收突發性的惡意流量攻擊，不額外收費

建置上線時間(on boarding) 短

Always on的全球大規模節點，提高服務效能

全球節點皆為全功能(Full Function)，不會有多節點連線產生的延遲時間

簡易使用的操作介面，減少維運成本

可使用API 介接，配合客戶客製化需求

自建的資安研發團隊，非與第三方購入資安數據庫

DNS 領導廠商，DNS 速度業界最快

## 認證與合規性資源

ISO 27001:2013

ISO 27701:2019

ISO 27018:2019

SOC 2 Type II

PCI DSS 3.2.1

C5:2020

樂雲服務

## 企業客戶選擇Cloudflare

完整的解決方案

可調整的網路規模

易於設定的統一操作介面

共享的即時情報

適合開發人員

支援多雲架構

## Cloudflare 企業客戶專屬方案

### 24/7/365 Global Support

- 專責客戶和技術工程師、IM專人服務 7x24立即回應
- 專人協助系統初始設定
- 全年無休的電話/電郵與線上交談支援
- 保證100%運作時間SLA

### 100% Tailor Made Solution

- 企業級抗DDoS無限防禦，DDoS吃到飽，只算乾淨流量
- 台灣節點使用優先權
- 多使用者/角色型存取控制
- 進階WAF及無限數量自定規則集
- 通過國際認證

樂雲服務

# 為何選擇Cloudflare?

1.吸收突發性的惡意流量攻擊，不額外收費
2.建置上線時間(on boarding) 短
3.Always on的全球大規模節點，提高服務效能
4.全球節點皆為全功能(Full Function)，不會有多節點連線產生的延遲時間
5.簡易使用的操作介面，減少維運成本
6.可使用API 介接，配合客戶客製化需求
7.自建的資安研發團隊，非與第三方購入資安數據庫
8.DNS 領導廠商，DNS 速度業界最快

## Cloudflare 服務流程

**1.售前諮詢**
了解客戶需求，
提供完整建議

**2.客製規劃**
依客戶需求客製
化服務

**3.導入設定**
架構建置及優化

**4.技術支援**
提供技術諮詢服務

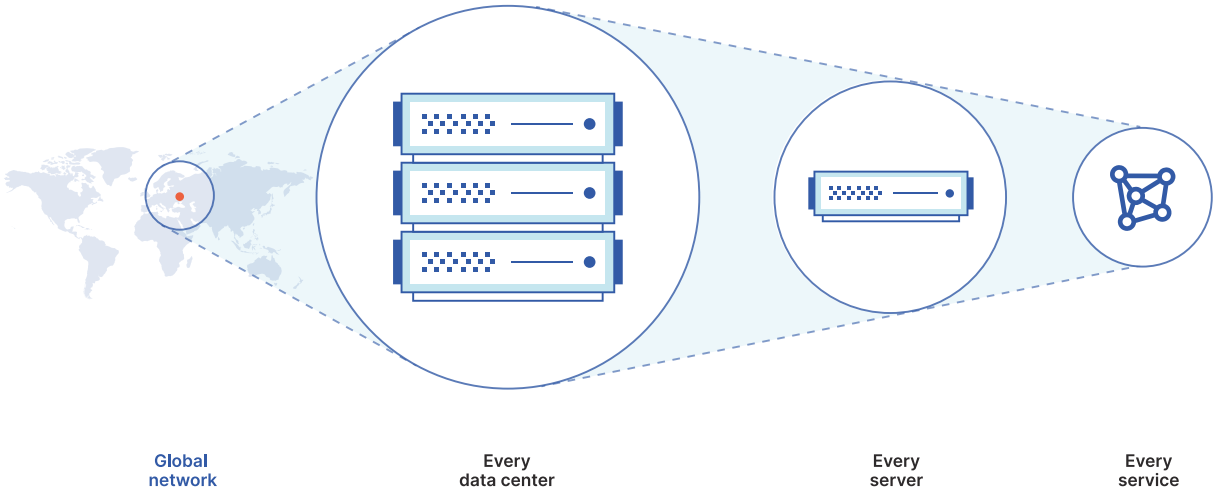
**5.售後維運**
7x24 全天候監控、
報修及維護

# Internet

對您的業務至關重要！

# CLOUDFLARE的使命：
# 幫助建構更好的互聯網

Cloudflare 通過龐大的全球網路加速並保護連接到互聯網的一切資產，為其提供性能加速、安全防護、高可用性和數據智能服務。

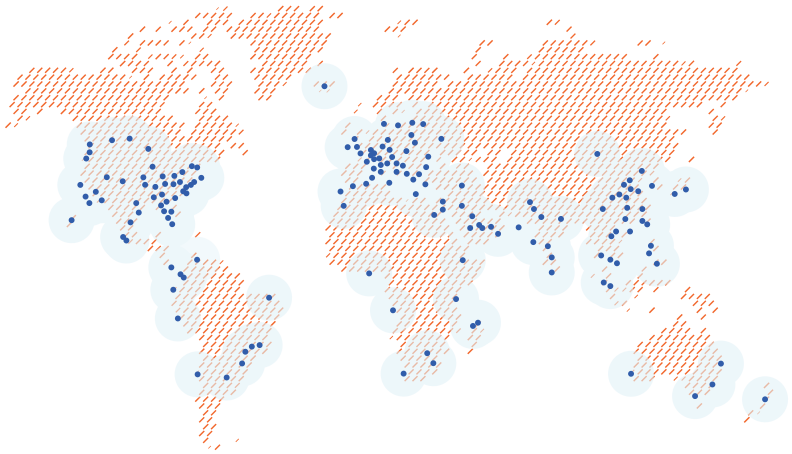


COMPANY PROFILE

# Cloudflare 公司簡介

## Cloudflare 全球網路

我們龐大的全球網路是地球上最快的網路之一，受到數百萬個 Web 資產的信賴。Cloudflare 網路與幾乎每一個服務提供者和雲提供商連接，與世界上網人口的 95% 連線速度不超過 50 ms。



| 節點 | ISP 線路 | 可用流量 | 低延遲 |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 285 個城市，遍布 100 多個國家和地區，包括中國大陸 | 11,000 個網路直連到 Cloudflare，包括所有主要 ISP、雲提供商和企業 | 192 Tbps 全球網路邊緣容量，包括傳輸連線、對等和私人網路互連 | 50 毫秒 95% 世界上網人口的網路延遲 |

COMPANY PROFILE

# Cloudflare 公司簡介

## Cloudflare

Cloudflare 保護並確保對外資源的可靠性，例如網站、API 和應用程式，還保護您的內部資源，例如防火牆幕後應用程式、團隊和裝置。這也是您用於開發全球規模應用程式的平台。

### 整合安全性與效能

深度整合的產品，形成統一的控制平台。

### 節點覆蓋

覆蓋超過 100 個國家/地區的 285 個城市的全球雲端網路

### 單一介面

無需變更代碼：CLOUDFLARE 儀錶板單一介面，可快速設定易於操作使用。

### 可程式化邊緣

在無需設定或維護基礎結構的情況下擴展現有應用程式或建立全新的應用程式。

# PRODUCTS & SERVICES

# 產品與服務

PRODUCTS & SERVICES

# 產品與服務

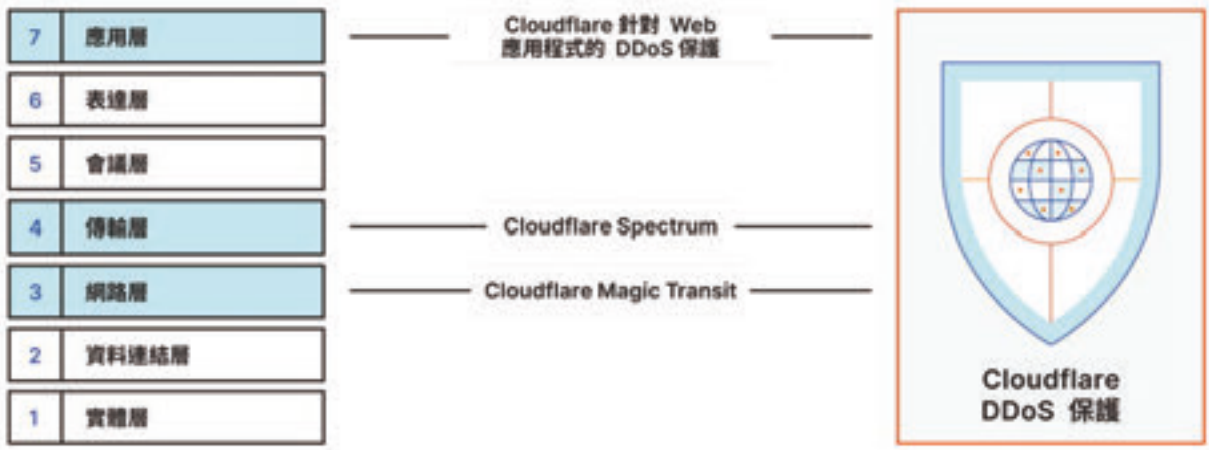
## 集成各種安全智能的應用和數據安全防護服務

CLOUDFLARE DDOS

# 防 護

## 為連線到網際網路的任何事物而建構

Cloudflare 提供三種 DDoS 保護解決方案，旨在保護您的雲端和內部部署網路上的一切。




### 專為 Web 應用程式而建構

在 Cloudflare 不斷更新的全球網路的情報支援下，為您的 Web 資產 (HTTP/HTTPs) 提供非計量的、永遠連線的 DDoS 保護。Cloudflare DDoS 保護與我們的雲端 Web 應用程式防火牆 (WAF)、機器人管理和其他第 3/4 層安全性服務協同工作，以保護資產免受各種網路威脅侵害。

### 為所有其他應用程式而建構

Cloudflare Spectrum 是一種反向 Proxy 服務，可為任何應用程式 (不僅是 Web) 提供 DDoS 保護，例如 FTP、SSH、VoIP、遊戲，或透過 TCP/UDP 通訊協定執行的任何應用程式。Spectrum 隨附內建的負載平衡和針對第 4 層流量的流量加速功能。

### 為網路基礎結構而建構

Cloudflare Magic Transit 是 Cloudflare 網路安全產品組合的組成部分，為網路基礎結構提供基於 BGP 的 DDoS 保護，可使用永遠連線或視需求部署兩種模式。遍佈 100 個國家/地區 285 個城市的資料中心宣告客戶子網路，以吸收網路流量並在靠近攻擊來源的位置緩解威脅。

CLOUDFLARE DDOS

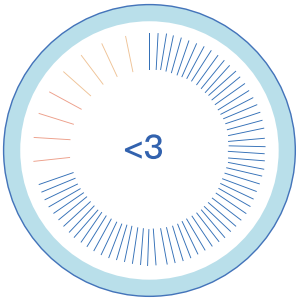
# 防 護

封鎖任何規模和種類的 DDOS 攻擊

## 以 Cloudflare 的規模緩解 DDoS

在 Cloudflare 跨越 100 個國家/地區 285 個城市的每個資料中心中，每一台伺服器都執行完整的 DDoS 緩解服務堆疊。

Cloudflare 的網路處理能力為 192 Tbps，可以很好地抵禦規模最大的攻擊。




快速緩解

## 位於邊緣的智慧型、自動化緩解措施

Cloudflare 集中化和分散式緩解系統彼此策應，在 3 秒以內聯合識別並緩解大多數 DDoS 攻擊。只需不到 1 秒，預先設定的靜態規則便可完成部署。

見吾知之所見

## 通過 GraphQL Analytics API 使數據民主化

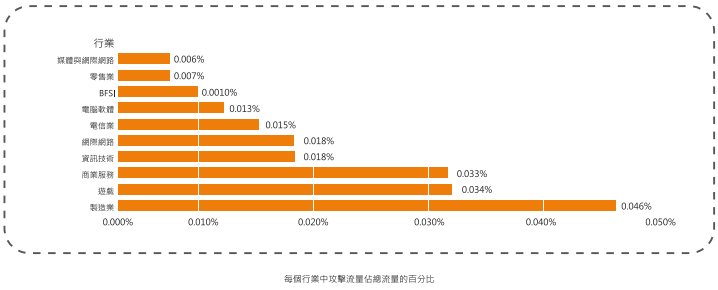
藉由 Cloudflare 內建分析功能，您可以從儀表板或透過 Cloudflare GraphQL API 更深入地瞭解您的流量模式、觀察到 (和已封鎖) 的威脅以及更多其他資訊。Cloudflare 日誌也可與協力廠商 SIEM 整合。

CLOUDFLARE DDOS

# 防 護

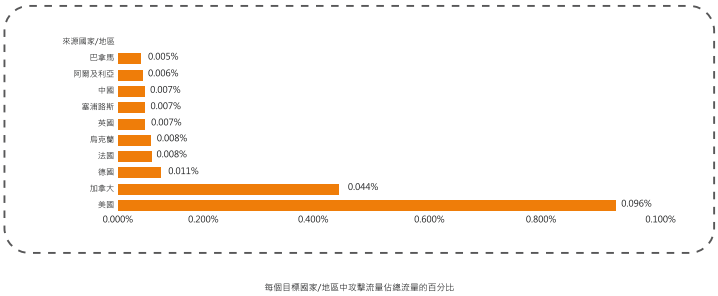
## 應用程式層 DDoS 攻擊: 行業分佈

按行業細分受到的應用程式層攻擊，可以發現在 2021 年第四季度，製造業、商業服務是受到攻擊最多的行業。



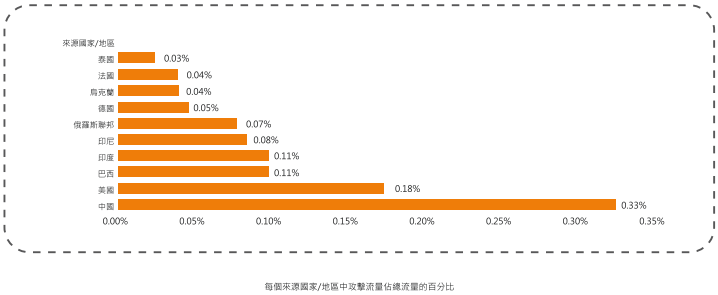

## 應用程式層 DDoS 攻擊: 目標國家/地區分佈

為確定哪些國家/地區遭受最多的 HTTP DDoS 攻擊，我們按客戶的帳單國家/地區對 DDoS 攻擊進行了分類，並以其佔據所有 DDoS 攻擊數的百分比進行表示。位於美國的企業今年連續第三次成為 HTTP DDoS 攻擊的最大目標，其次為加拿大和德國。




## 應用程式層 DDoS 攻擊: 來源國家/地區分佈

為瞭解 HTTP 攻擊的來源，我們研究了產生攻擊 HTTP 請求之用戶端的來源 IP 位址地理位置。與網路層攻擊不同，HTTP 攻擊中的來源 IP 位址無法偽造。特定國家/地區的高 DDoS 活動百分比通常表明大型殭屍網路在其境內運行。




中國是 DDoS 攻擊百分比最高的國家，已連續第四個季度位居榜首。每一千個源自中國 IP 位址的 HTTP 請求中，就有超過三個是 HTTP DDoS 攻擊的一部分。美國仍然佔據第二位，之後是巴西和印度。

# CLOUDFLARE WAF

2021 年，可供利用的漏洞超過 2 萬個，創下歷史紀錄。

暗網上有超過 50 億條被盜憑證，助長導致帳戶接管的憑證填充攻擊。

攻擊者瞄準了 Web 伺服器，使它們成為受到攻擊最多的 IT 資產，占攻擊總數的 50%。

公司修補漏洞需要長達 16 天，讓攻擊者有機可乘。

## WAF 分層防禦

- Cloudflare 託管規則提供進階零時差漏洞防護。
- 核心 OWASP 規則封鎖常見「前 10 種」攻擊技術。自訂規則集提供定制保護，以封鎖任何威脅。
- WAF ML 透過偵測繞過以及 XSS 和 SQLi 攻擊的變體，彌補了 WAF 規則集的不足。
- 暴露的認證檢查監控並封鎖使用被盜/被暴露認證接管帳戶。
- 敏感資料偵測對包含敏感資料的回應發出警示。
- 進階速率限制防止濫用、DDoS、暴力破解嘗試以及以 API 為中心的控制。
- 靈活回應選項允許封鎖、記錄、限速或質詢。

### 1 阻止帳戶接管

防止憑據填充攻擊成功接管用戶帳戶。

### 2 預防數據滲漏

阻止數據泄露，保護企業數據的安全和私密。

### 3 阻止憑證填充攻擊

檢測並阻止利用被盜憑據的登錄攻擊。

CLOUDFLARE
# WAF

## Cloudflare 的世界級應用程式安全

Cloudflare web 應用程式防火牆（WAF）是我們高級應用程式安全產品組合的基礎，這些產品確保應用程式和 API 安全、高效，抵禦 DDoS 攻擊，控制自動程式，檢測異常和惡意負載，同時監測瀏覽器供應鏈攻擊。

### 機器人管理

防禦損害 Web 資產的自動程式攻擊，提供卓越的用戶體驗。

### API Shield

通過 API 發現、模式驗證、mTLS、DLP、異常檢測等，使 API 安全並高效工作。

### Page Shield

防禦在訪問者瀏覽器中執行的第三方 Magecart 攻擊。

## Cloudflare 安全領導力

Cloudflare 榮獲 2022 年 Gartner Peer Insights™ CDN 和 WAAP 客戶之選稱號。

Frost & Sullivan Frost Radar ™：全球整體 web 保護市場報告中的創新領導者。

Forrester Wave DDoS 防護解決方案 “領導者”

CLOUDFLARE
# DNS

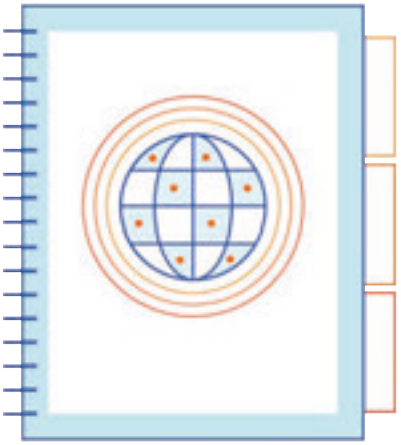
## 迅速、安全和具備復原能力的 DNS

DNS 是一款用於所有線上業務的關鍵任務元件。然而該元件常常被忽視和忘記，直到出現故障。

Cloudflare 的 1.1.1.1 是全球最快、最可靠的公共 DNS 解析器。

Cloudflare DNS 是一款企業級權威性 DNS 服務，可以提供最快的回應時間、無與倫比的備援以及採用了內建 DDoS 緩解和 DNSSEC 的進階安全性保障。

超過 10% 的網站將 Cloudflare 用作反向 Proxy。



## Cloudflare 的不同之處

**隨時可用**
我們的全球 Anycast network (任一傳播網路) 允許 285 個城市的每個資料中心在網路邊緣獲得 DNS 解決方案，藉此實現無與倫比的備援和 100% 正常運作時間。

**整合安全性**
Cloudflare 提供內建 DDoS 保護和一鍵式 DNSSEC，以確保您的應用程式始終獲得保護，以免受到 DNS 攻擊。

**一流效能**
我們的權威性 DNS 是世界上速度最快的，可以達到 11 毫秒的平均 DNS 查詢速度和低於 5 秒的全球 DNS 傳播。

**全球連線**
相較於全球其他提供者，Cloudflare 連線至更多網際網路交換。

# CLOUDFLARE DNS

## 無限 DDoS 防護

讓您的機構避免受到因 DDoS 攻擊而給您的 DNS 帶來的成本和壓力。有了 Cloudflare 受管理 DNS，您就相當於獲得了無限和非計量緩解，可對抗基於 DNS 的 DDoS 攻擊。我們的網路處理能力比有史以來最大的 DDoS 攻擊大 23x。

## 一鍵式 DNSSEC

Cloudflare 受控 DNS 採用內建 DNSSEC，可保護您的使用者避免受到在途攻擊，從而偽造或劫持您的 DNS 記錄。DNSSEC 在 DNS 查閱流程的每個層級都增加了一層額外的安全性屏障。更方便的是，您可以一鍵式輕鬆部署 DNSSEC。

## 由 24/7/365 技術支援提供保障，藉此輕鬆設定

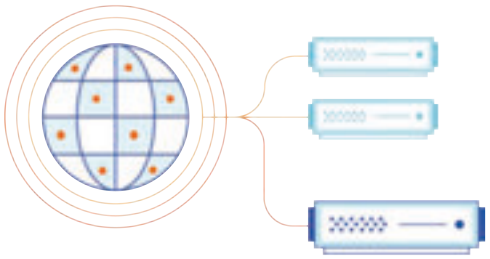
我們讓 DNS 變得簡單。無論您的產權在何處代管，您的所有網域都可以透過我們的使用者友善介面或 API 進行管理。Terraform 整合進一步實現自動化的 DNS 管理和設定。

您可以全天候獲得電話和電子郵件支援，並有工程師為您提供專門解決方案，助您取得成功 - 有助於採用和設定 DNS 記錄，實現零故障。

# CLOUDFLARE DNS

## 全球和當地負載平衡

樂雲借助 Cloudflare 負載平衡，您可以將流量從不正常的來源伺服器上移開，並以動態方式將其分配到可用性最高、回應速度最快的伺服器集區中，從而降低延遲和提高應用程式可用性。 我們的負載平衡解決方案利用了 Cloudflare 的全球 Anycast network (任一傳播網路)，並支援 HTTP(S)、TCP 和 UDP 等所有通訊協定。



## Advanced Analytics (進階分析)

對於您的 DNS 流量的健康程度進行深入即時分析 - 您可以從 Cloudflare 儀表板輕鬆獲得。針對您的 DNS 問題產生詳細的原始視覺化報告 - 可以透過回應代碼、記錄類型、地理位置、網域等項進行篩選。原始日誌文件也可以通過 API 獲得，並且也可以與 SIEM/解析工具集成。

## 快速配置電子郵件安全 DNS 記錄

讓您高枕無憂，通過我們簡單易用的電子郵件安全 DNS 嚮導，預防惡意行為者冒充您的網域發送欺詐電子郵件——配置所需的電子郵件 DNS 記錄僅需點擊幾下滑鼠。如果我們檢測到缺失或存在不安全的電子郵件配置，我們將向您發出警告。

CLOUDFLARE

# Zero Trust 平台

## 無論是遠程辦公，還是在辦公室，都能為使用者提供增強的安全性和一致的體驗

1. 通過在一個專門構建的全球網路上將網路連接服務與零信任安全服務結合起來，Cloudflare One 支援安全訪問服務邊緣（SASE）。
2. 放棄成本高昂的專有電路，代之以提供內置零信任功能、DDoS 緩解、網路防火牆和流量加速的單一全球網路。
3. 無需 VPN，即可安全、簡單地連接到資源。阻止橫向行動、勒索軟體、惡意軟體和網路釣魚。

### 具有彈性的簡單架構

快速追蹤您的歷程，以保護任意連線性。Cloudflare 使用單一網路和控制平面，來統一連線和保護端對端連線。

### 深受信賴的安全連線

確保可靠且可擴充的網路連線能力，隨時隨地提供一致的保護。使用相同的 Cloudflare 代理(其會路由所有網站約 20% 的流量)，為企業提供 Zero Trust。

### 更快速的未來創新

提前滿足現代企業需求，確保未來安全無虞。Cloudflare 以快速構建及交付而聞名於世，能夠以快速且原生的方式採用新的網際網路和安全標準。

## 實現 Zero Trust 之旅安全性現代化

**確保進出企業的所有流量都經過驗證並獲得授權。檢查動態環境，對每個要求「從不信任，始終驗證」。**

### 零信任網路存取（ZTNA）

對存取您所有應用程式的使用者強制執行預設拒絕（Zero Trust 規則），比 VPN 更快速且更安全。

### 安全 web 閘道（SWG）

保護並檢查企業網際網路流量，協助防止網路釣魚、勒索軟體和其他網際網路風險。

### 遠端瀏覽器隔離（RBI）

在遠離端點的位置執行程式碼，在不犧牲效能的情況下提供網際網路威脅防護並保護資料。

### 雲端存取安全性代理程式 (CASB)

輕鬆地保護 SaaS 工具、精細地控制使用者存取，並保護敏感性資料。

### 雲端電子郵件安全性

先發制人地保護您的使用者，使其免受網路釣魚、企業電子郵件入侵 (BEC) 和電子郵件供應鏈攻擊。

### 資料丟失預防 (DLP)

檢查 HTTP/S 流量中是否存在敏感性資料（如 PII），並使用允許或封鎖原則防止外流。

CLOUDFLARE
ONE

# Cloudflare One 的工作原理

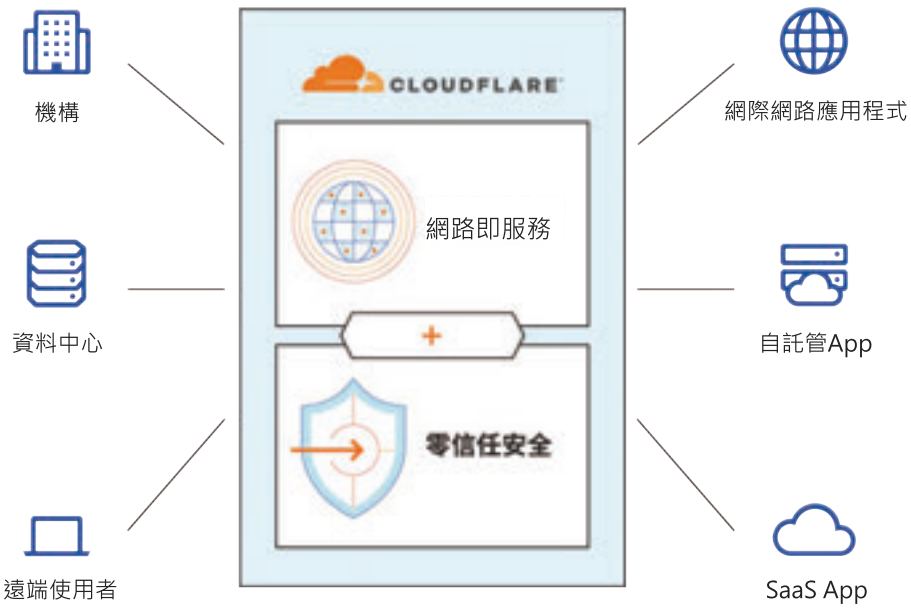
## Cloudflare Zero Trust 服務

ZTNA：透過強制執行基於身分和情境的規則，以比 VPN 更快且更安全的方式讓任何使用者連線至任何應用程式和私人網路。

CASB：針對 SaaS 應用程式的可見度和控制程度，以便阻止資料外洩、違反合規性、內部人員威脅、影子 IT 及危險資料共用等各種情況。

SWG：透過強制執行 DNS、HTTP、網路及瀏覽器隔離規則，封鎖已知和未知的網際網路威脅，並輕鬆控制資料流。

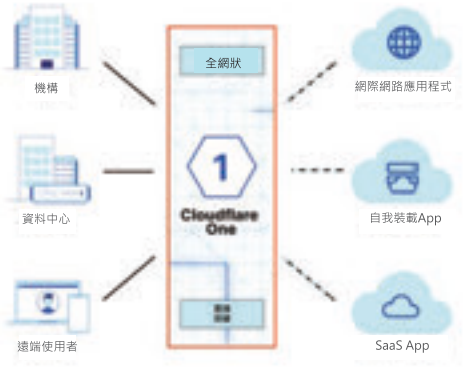
- 使用電子郵件安全和 DNS 篩選，獲得更強的威脅防護。
- 使用遠端瀏覽器隔離和 DLP，獲得更強大的資料保護。
- 使用身分識別 Proxy 和裝置狀態，實行更強的存取控制。



# CLOUDFLARE ONE

## Cloudflare One

不再使用緩慢的 VPN 和昂貴的 MPLS。Cloudflare 幫助團隊在網際網路的邊緣運行企業網路。我們遍佈 285 多個城市的龐大網路總是接近您的使用者，無論他們身處何地。




## 為何選擇 Cloudflare

### 部署和管理簡單輕鬆

每項 Cloudflare 服務都在我們遍佈全球 285 多個城市的資料中心之一上運行。不必為了採用 SASE 模型而手動集成多個獨立的產品。

### 在世界任何地方獲得一致的安全性和速度

每一個 Cloudflare 資料中心都能提供一次通過流量檢查和路由，為世界任何地方的使用者提供相同的保護，不會因為延遲而犧牲速度。

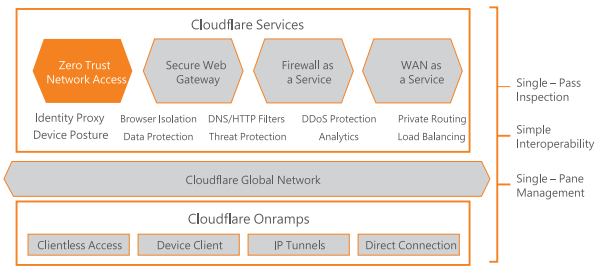
### 連接到原有服務

Cloudflare 運營世界上最強大、對等連接最多的網路，Cloudflare One 支援已經在使用的身份、端點和雲提供商。使用簡易，一次集成。

## Cloudflare One 的工作原理

### 零信任網路存取

通過執行基於身份和上下文的規則並限制橫向行動，比 VPN 更快、更安全地將任何使用者連接到任何應用程式和私人網路。



# CLOUDFLARE ONE

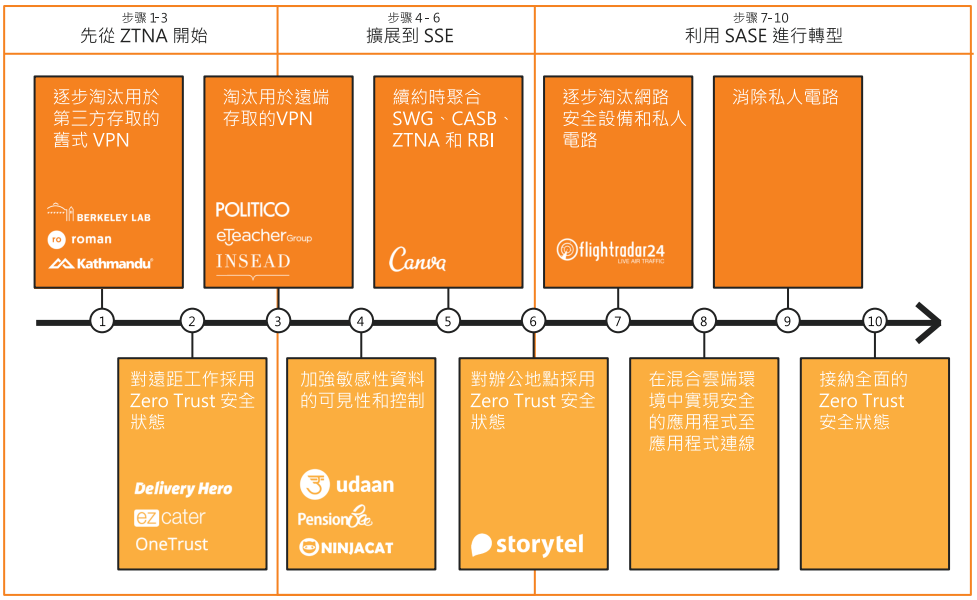
## SASE 之旅:實施安全存取邊緣服務，Cloudflare 保護和簡化您的網路

樂雲相信 Cloudflare One 與 Gartner 的 SASE 架構十分契合，可以從頭開始構建，並將 Zero Trust 安全平台與網路即服務產品進行原生整合。 Zero Trust 平台與 Gartner 的 SSE相合，並可聚合原本彼此相異的點式產品: ZTNA、VPN、SWG、 DNS 篩選、CASB、RBI 以及防火牆即服務 (FWaaS)。預設包含 DDoS 防禦，還能以附加服務形式添加雲端 WAAP，這些皆是 Gartner Hype Cycle報告中談到的相鄰市場。

您可以從僅使用 Cloudflare Access 來啟動 ZTNA 之旅。以後做好準備時，Cloudflare 會幫助您以高成本效益的方式輕鬆擴展到 SSE 或利用 SASE 進行轉型。

所有 Cloudflare 服務均在龐大的全球網路上每一資料中心內的每一伺服器上執行，因此不存在涵蓋缺口或不一致之處。在 285 個城市提供單遍檢查和單一窗格管理並實現 100% 正常運作時間 SLA，確保最高水準的安全性、效能和可靠性。

所有服務使用相同的網路入口 (例如裝置用戶端)，實現快速部署；採用相同的 UI 和基於 API 的原則管理，提升了易用性；還有相同的第三方身分識別、端點和雲端整合，最大化利用現有的投資。




"迅速擴展和提升遠距工作者使用者體驗的需求在採用和整合雲端網路安全控制中發揮重要作用，促使 SASE 和 ZTNA 等日漸興盛。"

Gartner

CLOUDFLARE

# SPECTRUM

## Cloudflare Spectrum

網際網路不僅僅是網路。它包含許多其他與 Web 服務具有相同基本需求的 TCP / UDP 應用程式——都需要速度、安全性和可靠性。

**Cloudflare Spectrum 是一種反向代理產品，可將 Cloudflare 的優勢擴展到全部 TCP/UDP 應用程式。**

### 速度

即時加速以解決網路擁塞

### 安全

具有超過 192 Tbps 緩解容量的 DDoS 防護

### 可靠性

具有快速容錯移轉的全域和本地負載平衡

CLOUDFLARE
SPECTRUM

# 遊戲專屬 Cloudflare Spectrum

## 保護並加速您的遊戲平台

1. 以線上遊戲平台為目標的巨流量 L3 和 L4 分散式阻斷服務 (DDoS) 攻擊無論是在頻率還是強度上都與日俱增。遊戲平台倘若 Ping 時間過長或服務完全不可用，會引起憤怒的使用者在社群媒體大發牢騷，造成品牌形象受損和業務損失。

2. DDoS 攻擊會威脅到全天候可用性和快速效能，而這兩項正是您線上互動式遊戲平台的立足基礎。

3. Cloudflare Spectrum 可保護在遊戲平台上運作的 TCP 和 UDP 應用程式免受 DDoS 攻擊，使其能在不影響效能的情況下保持線上狀態。

### DDoS 保護和 IP 防火牆服務

將遊戲基礎結構的 TCP 或 UDP 連接埠暴露給公共網際網路，會增加伺服器 IP 被揭露的可能性，因而容易受到巨大流量 DDoS 攻擊。

Cloudflare Spectrum 是透過 Cloudflare 的全球 Anycast Network來代理流量，因此攻擊流量會被分散到世界各地來吸收掉。Spectrum 整合了 Cloudflare 的 IP 防火牆，讓您能夠封鎖特定 IP 位址或整個 IP 範圍，使其無法連到您的 TCP 和 UDP 服務。

### 整合速度與安全性

您的線上遊戲顧客可能遍佈全球，而您遊戲伺服器所位於的地區可能與顧客相距甚遠，導致 Ping 時間過高。如果延宕明顯，或是遊戲回應速度讓人感到不夠『即時』，最終使用者就很可能會放棄遊戲。要想提供一流的使用者體驗，遊戲平台的速度至關重要。

Cloudflare 的分散式全球網路可為 TCP 和 UDP 應用程式阻絕威脅，卻不會有安全性相關延遲來造成效能降低。此外，面對 TCP 架構的服務，Cloudflare 會進行 TCP 最佳化並將 SSL 連線終端設在邊緣網路，不僅可以消除安全性相關延遲，還可以加快遊戲流量，達到『即時』的互動體驗。

### 輕鬆設定與擴展

一般來說，建置、維護及擴展客製化的安全性基礎結構來保護您的遊戲平台，不僅耗時又燒錢。此外，內部部署的傳統安全性設備並無法擴展至足夠規模來抵擋大量 DDoS 攻擊。

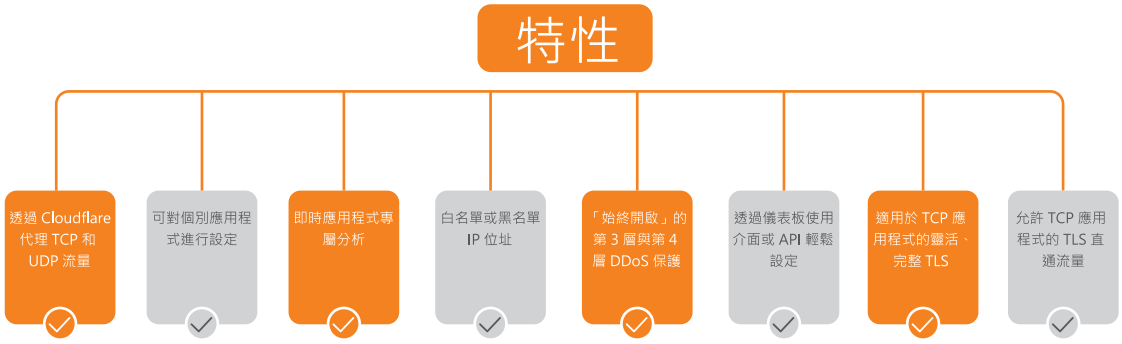
Spectrum 可在 Cloudflare 儀表板或 API 中針對個別應用程式來輕鬆設定，賦予您十足的控制權和靈活性。再搭配恢復力強的智慧型可擴展式網路，您就能抵擋最大、最新的攻擊，而無需投入大量工程資源來解決問題。

CLOUDFLARE

# SPECTRUM

Spectrum 產品發布之前，我們不得不依賴不穩定的服務和技術，而這些服務和技術又增加了延遲，因而影響了用戶體驗。現在，我們能夠在不增加延遲的情況下持續受到保護，這使 Spectrum 成為任何對延遲和正常運行時間敏感的服務（比如在線遊戲）的最佳選擇。

Cloudflare 的 DDoS 防護和 IP 防火牆不僅能保護網頁伺服器，還能延伸到其他 TCP 和 UDP 架構的服務，使其安全無虞地在線上運作。使用 Cloudflare Spectrum，讓您的遊戲 App 和服務享有全面的安全性與效能解決方案。




## 取得方式:

若要開始使用 Spectrum，可以聯繫樂雲業務團隊購買企業版 Spectrum。啟用 Spectrum 後，您就會針對非網頁 TCP 和 UDP 通訊協定與連接埠的部分，獲得加密以及巨大流量 DDoS 攻擊非計量緩解功能。

# Solutions

# 解決方案

全球網路優勢

# CLOUDFLARE TO GLOBAL

Cloudflare 正在幫助建設更美好的互聯網 —— 我們正在解決一些最重大的網路問題，建設更美好的互聯網。

在進行海外拓展時，使用 Cloudflare 網路來保護您的數據、最佳化網路速度並抵禦攻擊。

我們幫助您解決跨境運營中常見的問題：

1 -網頁加載時間過長，潛在客戶不勝其煩，轉化率下降

2 -全球業務拓展帶來的新攻擊威脅

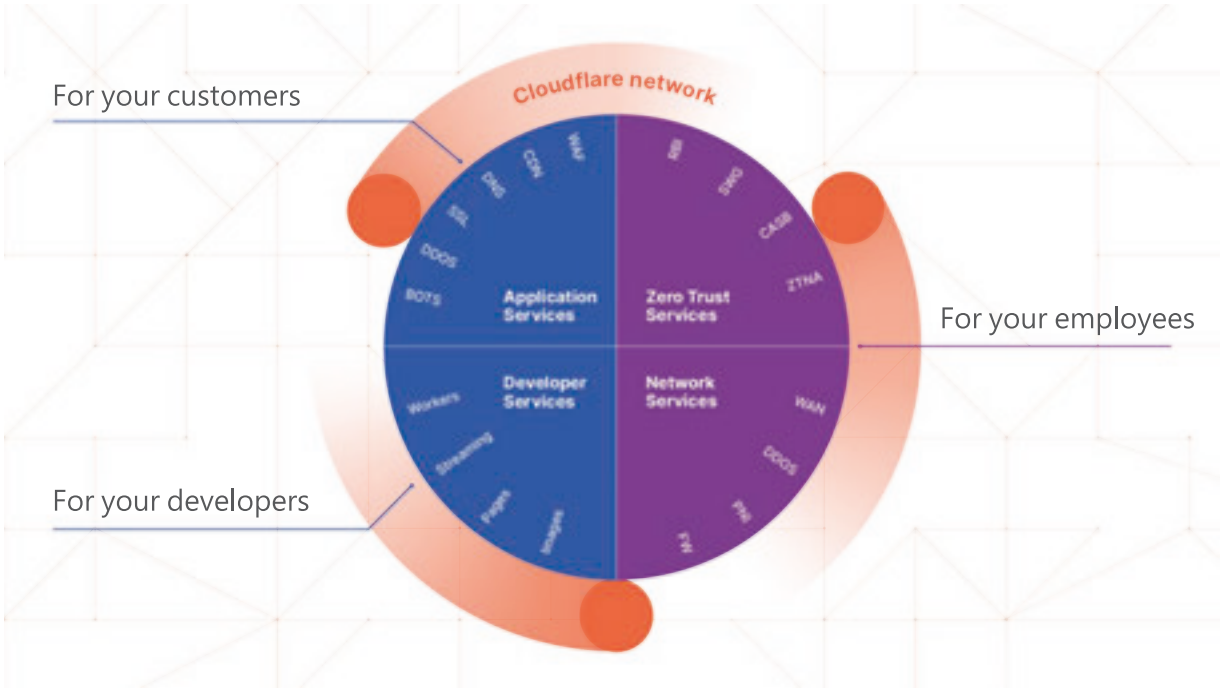
3 -數據傳輸問題有可能使數據面臨風險

全球網路優勢

# CLOUDFLARE TO GLOBAL

## 為雲而建的全球性網路

Cloudflare 是一個全球網路，讓您連接到網際網路的過程一切都是安全、私密、快速和可靠。




1 -保護您的網站、API 和網際網路應用程式。

2 -保護企業網路、員工和裝置。

3 -編寫和部署在網路邊緣運行的代碼。

CLOUDFLARE MAGIC TRANSIT

# 既保護網路，又提升效能

Cloudflare Magic Transit 為內部部署、雲端和混合網路提供 DDoS 保護和流量加速。憑藉遍佈 285 個城市的資料中心和超過 100 Tbps 的 DDoS 緩解容量，Magic Transit 能在接近源頭的位置偵測和緩解攻擊，平均用時不足 3 秒，而且還附帶了效能方面的效益。

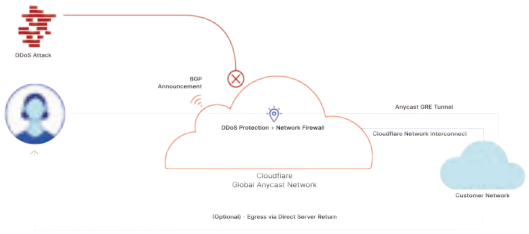
Magic Transit 是一個網路安全解決方案，從每一個 Cloudflare 資料中心為本地、雲託管和混合網路提供 DDoS 保護、流量加速和其他眾多功能。

CLOUDFLARE MAGIC TRANSIT

# 既保護網路，又提升效能

## 基礎結構架構的下一步

Cloudflare Magic Transit 可保護整個 IP 子網路免受 DDoS 攻擊，同時還可加速網路流量。它通過 Cloudflare 的全球網路來緩解攻擊，採用 BGP 、GRE和 IPSec 等基本網路通訊協定進行路由和封裝。您的所有網路資產，無論位於本地還是在私有雲或公共雲中，都會受到保護。




### 連線

使用邊界閘道通訊協定 (BGP) 路由通知到網際網路和 Cloudflare 的 Anycast 網路，客戶流量被接收到最靠近來源的 Cloudflare 資料中心。

### 保護和處理

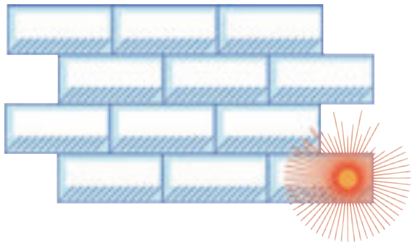
檢查所有客戶流量是否存在攻擊。可以在偵測到攻擊時立即套用先進的自動緩解技術。其他功能 (如負載平衡、下一代防火牆、內容快取和無伺服器計算) 也作為服務提供。

### 加快速度

乾淨的流量透過 Cloudflare 的網路進行路由，以獲得最佳延遲和輸送量，並可透過 GRE 通道、私人網路互連 (PNI) 或其他形式的客戶網路對等互連來提供。

## 選擇您的網路功能

Cloudflare Magic Transit 與我們一流的網路防火牆整合，允許您為 IP 範圍設定細微性允許/拒絕規則，並可在幾秒鐘內傳播變更。想要應用程式層級防火牆？設定可選的 TLS 終止並開始檢查有效負載。想要 Load Balancer？您都有了。想要編寫無伺服器的 Cloudflare Worker 來動態修改流量？您也能做到。Magic Transit 與 Cloudflare 的所有 L4 和 L7 產品以原生方式整合 。



## 流量加速

Cloudflare 網路平均每秒服務 4500 萬個 HTTP 請求。隨著我們每個位元的移動，我們的網路變得越來越智慧和快速。

與 Argo Smart Routing 整合後，Cloudflare Magic Transit 將使用最快、最可靠的連結向您的網路提供即時乾淨的流量。

CLOUDFLARE MAGIC TRANSIT

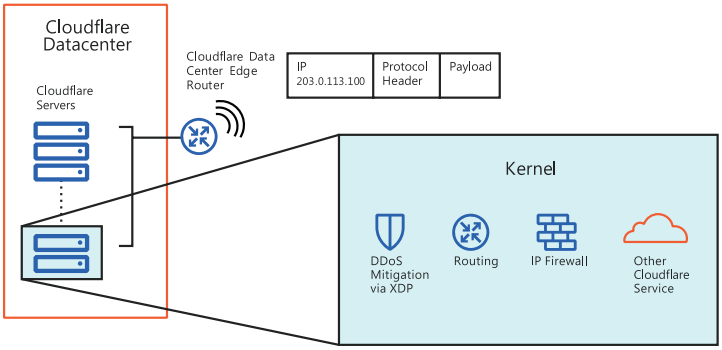
# 提供 DDOS 保護和流量加速

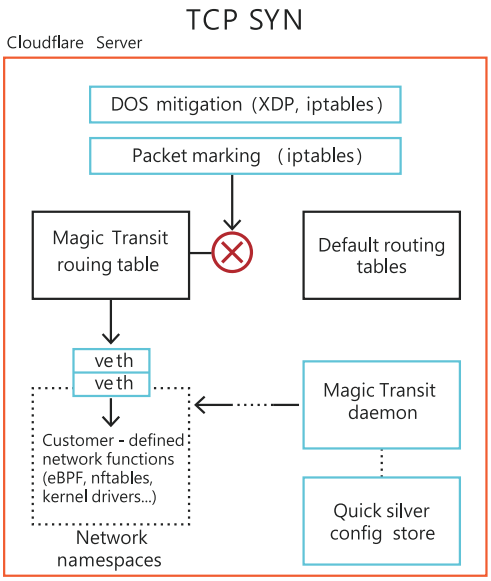
## 使用網路命名空間進行隔離和控制

在 Magic Transit 誕生之前，保護網路基礎結構免受 DDoS 攻擊的策略主要有兩種: 內部部署硬體 DDoS 防護設備和雲端清理解決方案。

在一定程度上，內部部署硬體設備可以妥善地保護您的基礎結構。但這些設備的頻寬有限，可能會被規模較大或同時發生的攻擊壓垮。硬體還需要大量前期投資，並耗費大量資源來管理和維護。

雲端清理中心應運而生，提供了一種更簡單的替代選擇:使流量經由清理中心進行路由，並在清理中心篩選掉攻擊流量。這解決了內部部署硬體引起的財務負擔和維護難題。




由於這些雲端提供者的清理中心數量有限，並且分散於不同的地理位置，因此流量可能必須傳輸很長距離進行清理，然後才能到達最終目的地。雲端提供者通常只有屈指可數的清理中心，如果您或最終使用者與所有清理中心都相隔甚遠，即使最終目的地就在附近，流量也必須傳輸很長一段距離。

CLOUDFLARE

# 讓您的遊戲平臺及出海遊戲業務安全快速

## 為何遊戲公司選擇 Cloudflare

Cloudflare 提供一整套效能、安全和可靠性解決方案，幫助保護和加速您的遊戲。

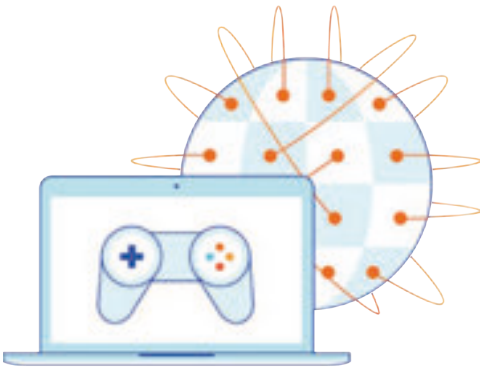
CLOUDFLARE

# 讓您的遊戲平臺及出海遊戲業務安全快速

## 使用 Cloudflare 網路保護和加速您的遊戲和玩家

Cloudflare 的網路覆蓋 100 多個國家的 285 多個城市，與全球 95% 上網人口的連線速度不超過 50 毫秒。 Cloudflare 服務可執行於我們網路中的每台伺服器上。這意味著:

1. DDOS 攻擊緩解在源頭附近進行，從而迅速回應
2. 靜態內容在接近玩家的地方快取，提供更佳效能
3. 威脅情報資料保護您的遊戲免受最新攻擊



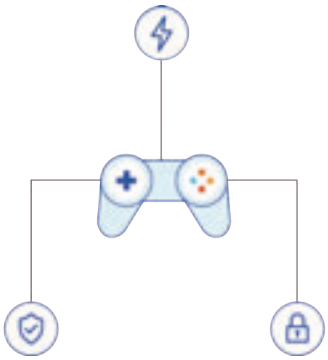
「 Cloudflare讓我們可以放心地專注在改進產品上，不用擔心API與閘道伺服器會遭受 DDoS 的攻擊威脅。」

Stanislav Vishnevskiy
Discord 技術長

CLOUDFLARE

# 讓您的遊戲平臺及出海遊戲業務安全快速

## Cloudflare 助您更上一層樓



未使用 Cloudflare 服務

各種產品的優先事項相互競爭，導致資料孤島並破壞效能。

使用 Cloudflare 服務

Cloudflare 產品原生整合，建立分層的情報而非讓步。

透過從單一儀表板管理的全球性網路，Cloudflare使您的遊戲保持連線，確保玩家低延遲體驗，同時保護您的智慧財產和玩家資料。

「只有 Cloudflare 提供的解決方案能同時保護我們網路的 L3 和 L4 層。 L3 層的 Magic Transit 與 L4 層的 Spectrum 相結合為我們的設定提供了理想的解決方案。」

Nicholas Herring
CCP Games 基礎結構技術總監

CCP

CLOUDFLARE

# 協助改善電子商務網站的安全性和性能

## 適用電商的 Cloudflare

### 增加購買人參與度

豐富的媒體和個人化可以展示您的產品和服務，但也可能會對頁面載入時間和響應速率造成負面影響。

### 防止詐欺活動

電商欺詐在近年來日漸頻繁，對零售商帶來顯著的銷售和盈利損失。

### 正常運作時間與可靠性

大型事件例如 DDoS 攻擊或是季度促銷活動會帶來顯著的流量暴增和故障。

### 降低營運成本

零售商比以前更加敏捷，並需要工具協助他們的網頁開發，讓工作更有效率，同時減少運營的人員和成本。

### 保護遠程工作團隊

通過無縫驗證，為任何用戶提供對內部應用的安全訪問，不受設備類型或位置限製。

### 在邊緣部署情報

通過在 Cloudflare 遍布 100 多個國家、285多個城市的網路上部署無服務器代碼，執行基於地理位置的訪問策略，降低延遲。

### 保護定製應用

保護需要一致正常運行時間和快速性能的業務關鍵型應用（非基於 HTTP）。

CLOUDFLARE

# 協助改善電子商務網站的安全性和性能

## 多媒體管理和最佳化

買家需要先參與和產品的互動，才能做出是否要購買的決定。高品質的影像和影片有助於展示您的品牌。

- 壓縮影像檔案以加快載入時間
- 從單一原始影像為行動裝置隨時調整影像大小
- 快取內容以將延遲時間降到最低
- 串流產品示範影片

## 最佳化驅動個人化內容的指令

根據買家的購買歷史或偏好來推送精準的內容，會增加他們購買的機率。構建動態網頁會增加載入的複雜性和時間。

- 透過 Argo 加速來自您來源網頁伺服器的動態內容請求
- 降低 DNS 解析時間
- 透過 Workers 無伺服器功能降低對來源的依賴性

## 防止欺詐活動

網路罪犯不斷使用更加複雜的方法在您的網站上執行詐欺交易和活動。Cloudflare 提供了一個穩健、安全的雲端式網路，可以最大程度地降低商店遭受詐欺活動的風險。

- 利用網頁應用程式防火牆 (web application firewall) 封鎖 SQL 資料隱碼攻擊和跨網站指令碼
- 為 PCI-DSS 保護敏感客戶資料
- 利用 TLS 1.3 加密所有客戶資料和交易

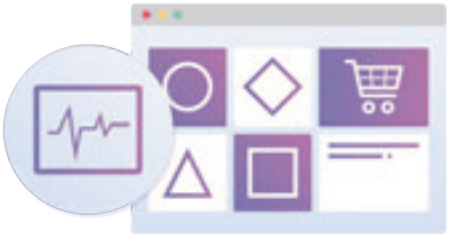
CLOUDFLARE

# 助力改善電子商務網站的安全性和性能

## 確保正常運作時間與可靠性

大規模事件例如 DDoS 攻擊，或是季節性促銷的流量頂峰，會為您的網頁基礎結構帶來壓力並可能引發故障。

- 抵禦由大型分散式阻斷服務（DDoS）攻擊帶來的故障
- 利用速率限制來防止來源基礎結構遭受過量負載，以緩解流量暴增
- 當出現伺服器故障時，在多個來源實現流量負載平衡




## 降低營運成本

電商讓零售商可以觸及更多買家，讓他們可以每天 24 小時全年無休為客戶提供產品和服務。設計和代管自己的電子商務網站的零售商正在尋找提高營運效率和增加盈利能力的方法。透過與頻寬聯盟代管提供者的合作，提供快取靜態內容並降低頻寬使用量。

- 利用 WORKERS 無伺服器功能降低伺服器成本
- 無需額外費用，保護網站網域註冊服務
- 利用原生 API 架構和 TERRAFORMS 整合來提升開發人員敏捷度

CLOUDFLARE

# 為金融行業保駕護航

## 金融業為何選擇 Cloudflare？

### 提供卓越的線上體驗

金融機構客戶都希望其線上平台能夠保證效能、便利性和可用性，即使在尖峰活動期間也不能受到影響。

### 緩解 DDoS 攻擊

利用快速、容易部署且可調整規模的分層式防護來抵禦 DDoS 攻擊。

### 提升敏捷性，降低營運成本

用基於雲端的服務取代傳統的基礎結構，縮短產品上市時間，並省下預算來用於創新。Cloudflare One 提供單一控制面板，供您管理Cloudflare 的多種安全與網路服務。

### 保護遠距工作團隊

無論使用者身在何方，使用什麼裝置，都能透過無縫身分驗證，讓所有使用者安全存取內部應用程式。

### 在邊緣部署情報

透過在 Cloudflare 遍布 100 多個國家/地區 200 多個城市的網路上部署無伺服器程式碼，實施基於地理的存取原則或降低延遲。

### 保護自訂應用程式

保護關鍵業務應用程式 (而非基於 HTTP 的應用程式)，使這些應用程式獲得一致的正常運作時間和快速效能。

CLOUDFLARE

# 為金融業提供最佳安全性

銀行業務正在發生迅速演變。數位時代的消費者很少依賴實際的分支銀行親身體驗，轉而選擇身臨其境的線上體驗。想要加速其數位轉化的銀行與投資服務公司需要在所有渠道和營運中提供卓越的客戶體驗。

Cloudflare 提供一種安全、具備復原能力的雲端網路，該網路可協助銀行與投資服務公司加速其數位轉換並提升營運體驗。

## 提高安全性

SSL 和加密是一項新規範，並且體現在網際網路中發生的任何交易或交換中。Cloudflare 在預設情況下是加密的，並提供服務陣列以確保合規。

### 1 防止 DNS 劫持

Cloudflare 是一種安全的網路，可防止客戶受到網路罪犯活動的攻擊。Cloudflare 提供的解決方案可提供 DNSSEC 以透過損壞您的 DNS 基礎結構防止將您網站中的消費者重新導向。

### 2 保護消費者資料

Cloudflare 透過其 Web Application Firewall 服務 (WAF) 提供對您的任何網際網路設備的第 7 層防護。Cloudflare 提供完全受控的 WAF 服務，該服務利用來自其支援的 1300 多萬個網際網路設備中的機器學習來識別可疑或惡意流量。

### 3 封鎖憑證填充嘗試

傀儡程式正在被日益部署以損壞客戶帳戶。Cloudflare 可識別各類模式，並根據已知傀儡程式流量模式將其進行對比以防止其存取您的應用程式。

## 提供更佳的客戶體驗

消費者花費了大量線上時間，您的網站也成為他們交互及使用您的服務的主要渠道。

### 1 頁面載入時間更快

Cloudflare是一種全球雲端網路，可快取我們任何資料中心的網站資產並縮短網頁內容的載入時間。圖片檔案可透過內建調整大小和壓縮演算法進一步最佳化。

### 2 輕鬆嵌入式視訊

促銷性視訊直播點播可在任何瀏覽器中輕鬆上傳和串流。

### 3 DDOS 防護

客戶銀行體驗的任何中斷都將必然造成體驗降級。DDoS 攻擊會造成故障，進而影響客戶滿意度。Cloudflare 的龐大網路能夠緩解大規模攻擊並使您的網站連線。

CLOUDFLARE

# 為金融業提供最佳安全性

## 增強開放式銀行業務

銀行業務需要透過日益多樣化的第三方服務陣列增強互操作性。銀行業務正在日漸從垂直導向模式(只需一家銀行即可完成所有作業)發展為更為水平傾向的開放式平台(整合多樣生態系統服務與應用程式的代管)。

### 1 加速 API 請求

Cloudflare 是一種適用於您的應用程式的安全的反向代理，並能緩解第三方 API 造成的大量請求流量，消除了任何潛在的效能瓶頸。

### 2 快速的智慧型流量路由

當 API 呼叫您的托管伺服器以獲得動態內容或資產時，Cloudflare 網路將經過調整以識別通向該使用者的最佳化路由，避免任何壅塞或故障。

## 提高行動裝置 App 的可靠性

消費者期待一種無縫式行動體驗，該體驗包括一項可靠的 APP 體驗。行動銀行業務在很大程度上成為許多使用者的規範，並可確保流暢的體驗。網路變化對消費者的行動體驗而言是一項挑戰。手機網路，還是手機與無線網路之間的切換，這些對您的使用者都可能具有破壞性。

### 1 更佳的網路連線

行動裝置開發人員可針對行動裝置 App 輕鬆合併 Cloudflare 的 SDK 以獲取對行動網路中其 App 效能的有價值的見解;包括特定區域的錯誤率和效能。

---

Cloudflare 使我們能夠推動技術前沿並快速、簡單地完成絕妙的事情。它確實是一項競爭優勢。

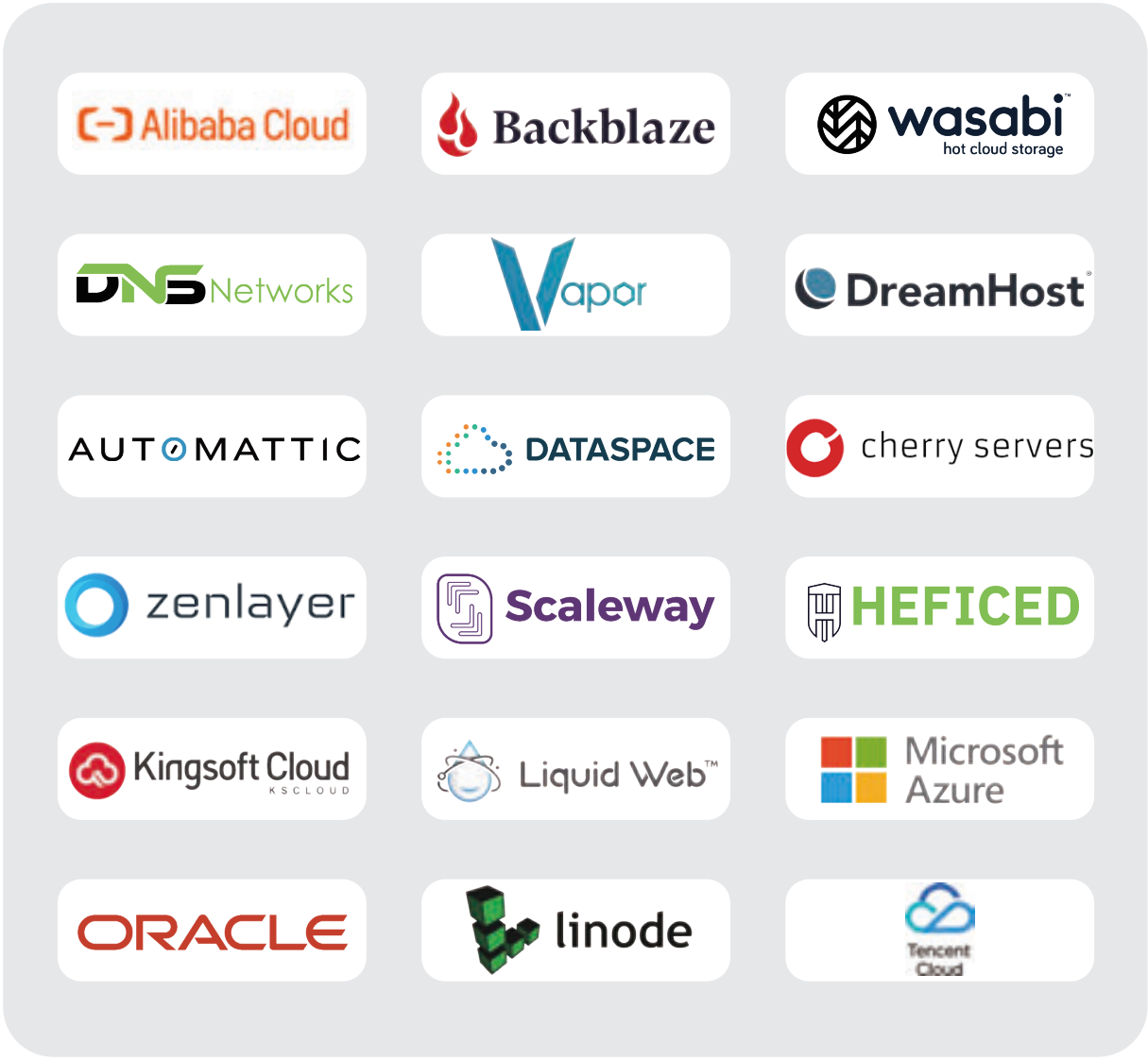
PAUL ABRAMSON
SVP/技術主任

主要成果:

- 70%頻寬節省
- 頁面載入時間縮短50%
- 符合.BANKTLD的產業法規 • 內建和自動化DNSSEC管理

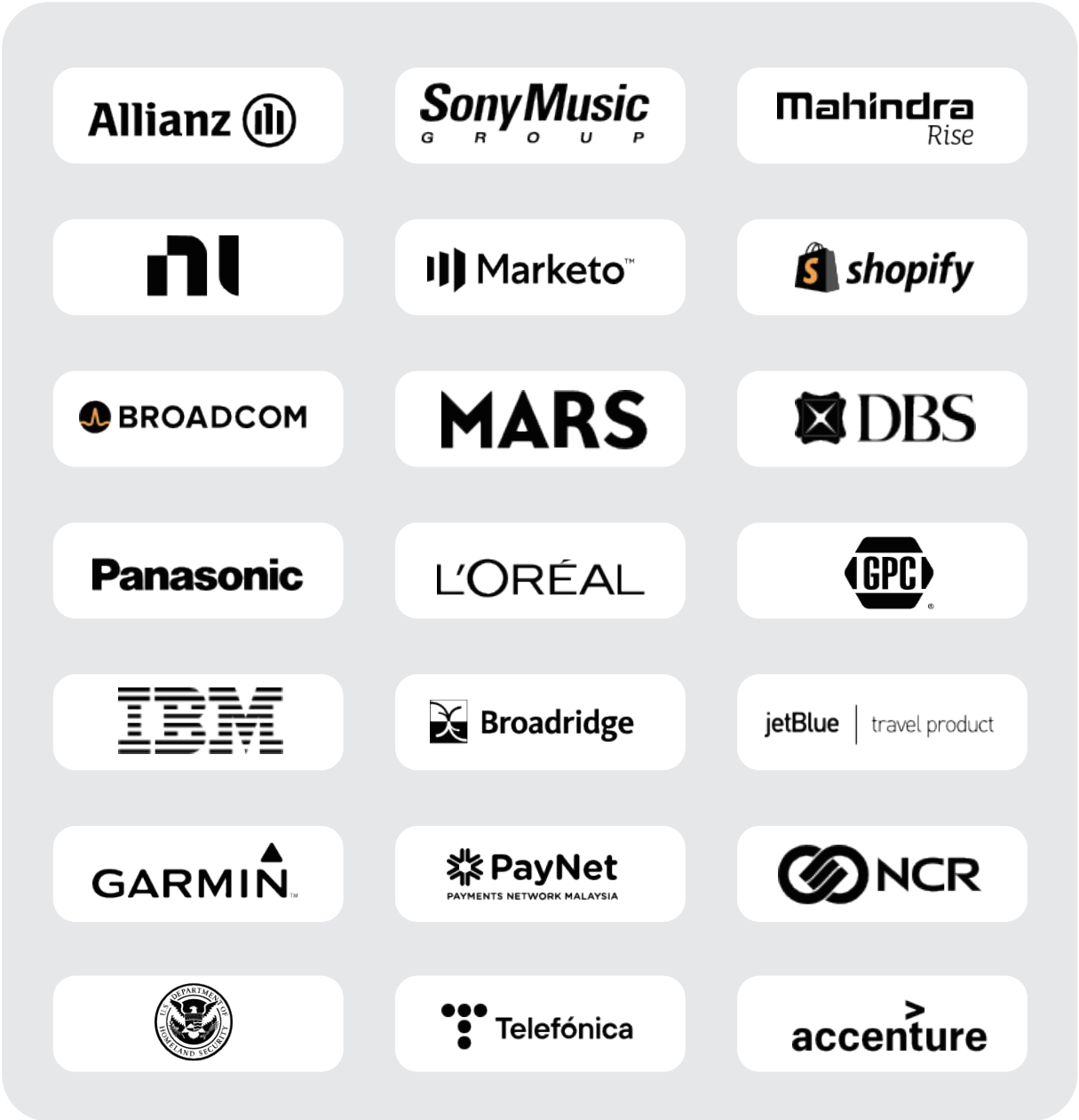
Montecito Bank & Trust

# Cloudflare全球頻寬合作商



# 使用Cloudflare的客戶

# 遷移到 Cloudflare 的企業



聯繫我們

# CONTACT US

樂雲為Cloudflare合作夥伴，使用Cloudflare服務，將Cloudflare擴展到您的所有網路

- 樂雲網站：https://www.leyun.cloud/
- 聯絡電話：+886 2-7722-0055



www.leyun.cloud

Line | @leyun

FB | Leyun.Inc

IG | Leyun.Inc