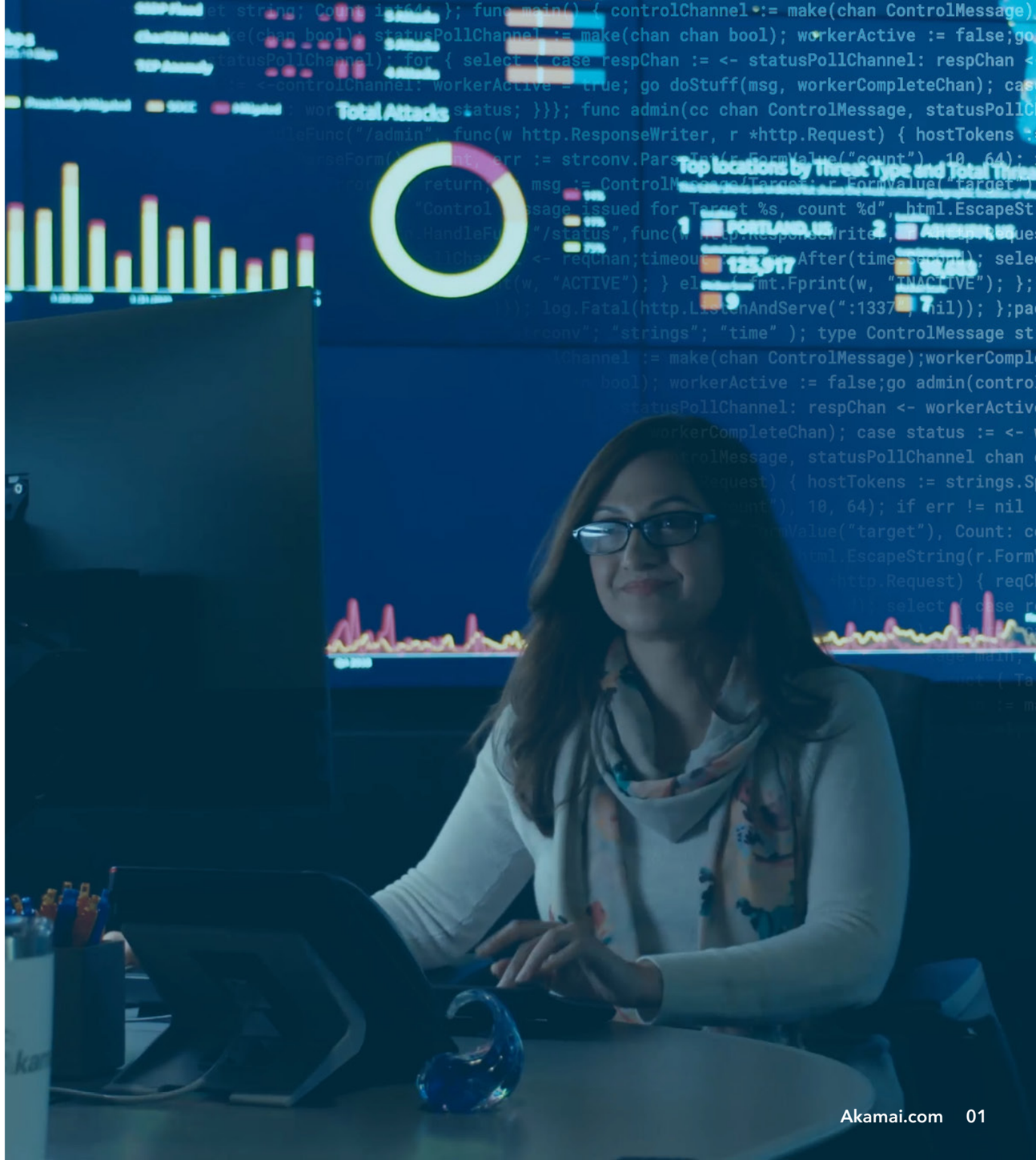
# 混合雲端時代的 DDoS 防禦

電子書

# 混合雲端時代的 DDoS 防禦

分散式阻斷服務 (DDoS) 是最古老的網路威脅類型之一，迄今仍是大規模干擾的常用工具，無論規模大小，幾乎每一種類型的企業都必須面對它帶來的安全風險。事實上，根據 IDC 的資料顯示，到 2023 年為止，DDoS 攻擊估計將以 18% 年複成長率持續增長，明確顯示著手加碼投資可靠的緩解機制已刻不容緩。雖然有些企業可能認為他們的 DDoS 攻擊風險低，但是當企業越來越依賴網際網路連線能力來驅動關鍵業務服務與應用程式，若疏於保護基礎架構，則可能導致大規模服務中斷和效能衰減。



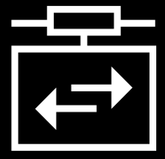
# 持續進化的威脅

DDoS 攻擊的規模每兩年就增加一倍，攻擊手法的變化與組合更呈現出前所未見的複雜性。而當應用程式與網路可用性成為業務持續性的關鍵，威脅發動者就有更多誘因發動流量型的通訊協定與應用層 DDoS 攻擊，試圖干擾任何可能存在的故障點，阻礙終端使用者存取網際網路上的資源和資產。

**DDoS 攻擊者會攻擊任何潛在故障點，例如：**

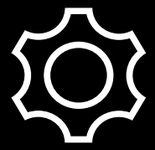
網站

網路應用程式
與其他企業服務



VPN 集中器遠端存取
企業資源

SD-WAN 控制器



應用程式開發介面 (API)

網域名稱系統 (DNS)
與原始伺服器

資料中心與網路基礎架構

藉由偵察這些受害環境、應用程式和 IP 空間，攻擊者就能判斷哪些 DDoS 手法會對網際網路服務和原始伺服器託管基礎架構造成最大的損害。也由於入行門檻降低，威脅發動者擁有豐富的攻擊技術與工具 (例如租用型的當機攻擊與 DDoS 攻擊等服務)，幫助他們找出企業防禦上的弱點或漏洞。

> 威脅發動者的動機各不相同，例如勒索和金融操作。Akamai 發現勒索行動範圍不再侷限於金融產業，已經開始鎖定商業服務、遊戲、旅遊餐旅、高科技、物流和零售等產業。
>
> – Roger Barranco
> Akamai 全球安全營運副總裁

**企業致力於擴張及保護遠端存取能力，試圖確保員工生產力與業務運作如常之時，DDoS 攻擊的衝擊也會同時加大。**

# DDoS 攻擊的後果

如果是網路層 (第 3 層) 和傳輸層 (第 4 層) 攻擊，就會利用流量型和通訊協定型的攻擊，試圖堵塞網際網路通道，癱瘓伺服器，並占用狀態記錄空間，使網路和服務無法使用。若是應用程型 (第 7 層) 的攻擊，威脅發動者則會透過低流量慢速攻擊和 HTTP 洪流等攻擊手法，試圖干擾網路效能和使用者體驗，進而造成系統停機，損害企業獲利。

然而，停機帶來的影響遠遠超出攻擊目標服務和應用程式無法使用的代價。***據 Ponemon Institute 指出，企業遭受 DDoS 攻擊所承擔的年平均損失為 170 萬美元***，其中即包括了技術支援成本增加、案件應變資源耗費、內部提報成本、法務成本、營運中斷以及員工生產力的損失。

顯然 DDoS 攻擊影響甚鉅，而在產業大舉移轉混合雲端基礎架構的當下，影響更不減反增。

# 雲端使企業的安全狀態持續複雜化

隨著企業開始淘汰傳統資料中心，將應用程式移轉雲端託管的環境，安全架構也變得更加複雜。許多企業雖想為連線網際網路的資產提供可比擬資料中心內部資源的 DDoS 防護，卻不知如何進行。此外，因為企業無法直接控制雲端託管的 IP，更增添了複雜性；一旦未妥善保護，很容易就遭受 DDoS 攻擊。

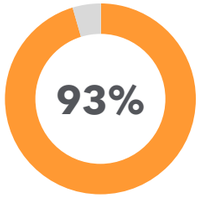
而威脅發動者也清楚知道業界正加速移轉共置設施和公用雲端。不一致的安全性原則與需求使企業安全架構和狀態產生弱點，異質而凌亂的雲端託管基礎架構也使得疑難排解作業更加困難，這些都是威脅發動者迫不及待想要利用的情況。

**結論：**

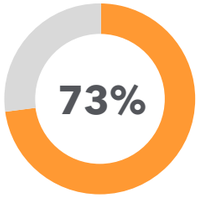
現代企業需要自適應的防禦機制，才能保護各式各樣的網站資產與服務，無論架設於何處。此外，超過 93% 的企業 (員工人數 1,000 人以下) 採用多雲端策略，使得消弭基礎架構複雜性所帶來的防禦缺口變得更加迫切。[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

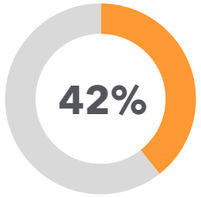
公用雲端環境內的安全責任，視供應商而異，而許多企業則誤作假設而使自己暴露在風險之中。例如一份 IBM 問卷調查發現，有 73% 的企業受訪者認為軟體即服務 (SaaS) 的安全防護主要責任在於 CSP (公用雲端服務供應商)，42% 認為雲端基礎架構即服務 (IaaS) 的安全防護主要責任在 CSP。這種安全控管責任歸屬不明確的情況就可能遭到入侵，也沒有任何企業願意接受此風險。




的企業採用多雲端策略




的受訪者認為公用 CSP 應負責保護 SaaS 安全




的受訪者認為 CSP 應負責保護雲端 IaaS 安全

Forrester 在近期一份白皮書指出，大多數企業選擇混合雲端策略，使用多家公用雲端供應商搭配內部部署的工作負載。有鑑於此，該分析公司建議選擇能夠保護混合架構的 DDoS 緩解服務供應商。


**威脅發動者只要猜對一次便已足夠。企業需要反應靈敏的緩解控制才能有效反擊。**

# DDoS 緩解方案並非都一樣有效

如今業界持續投資雲端基礎架構，想要在混合環境中確保一致的控管機制，卻仍是資安團隊一大挑戰。而當部署於多重後端雲端基礎架構的應用程式變得更難保護，許多企業開始希望能經由單一控制點來協調所有防禦。如今安全技術堆疊日益複雜，許多人也同樣渴望擁有一套單一管理介面：不僅能最佳化可見度，更能精簡化報告功能，直接使用 API 傳送給事件資料關聯分析系統。

***為解決此問題，越來越多企業轉向雲端型 DDoS 安全服務的供應商，幫助推動混合雲端的移轉策略。他們想要具規模彈性且反應靈敏的防禦機制，能保護位於任何位置的企業服務。***而其原因正是因為 CSP 的環境獨特，導致 DDoS 防護措施的整合、部署與管理作業複雜性增加。當越來越多連線網際網路的資產分散在多重雲端之間，更導致複雜性快速增長。

不但如此，許多 CSP 內部的 DDoS 緩解解決方案均缺乏關鍵能力，如可見度、SLA 和報告，這些都是當今的企業資安人員所需的重要功能。

對資安團隊而言，可見度與可據以行動的見解就是一切，能讓團隊最佳化事件回應及妥善度。有些 CSP 的 DDoS 解決方案報告、可見度和攻擊事後分析幾乎不透明，也難怪許多人稱 CSP 為分析與報告的黑盒子。

甚至有些 CSP 不提供緩解時間 SLA，僅向受影響的企業提供服務抵扣點數。當每一秒都可能是成敗關鍵，企業需要能保障服務供應商在不影響效能的情況下，維持系統運作和可用性。

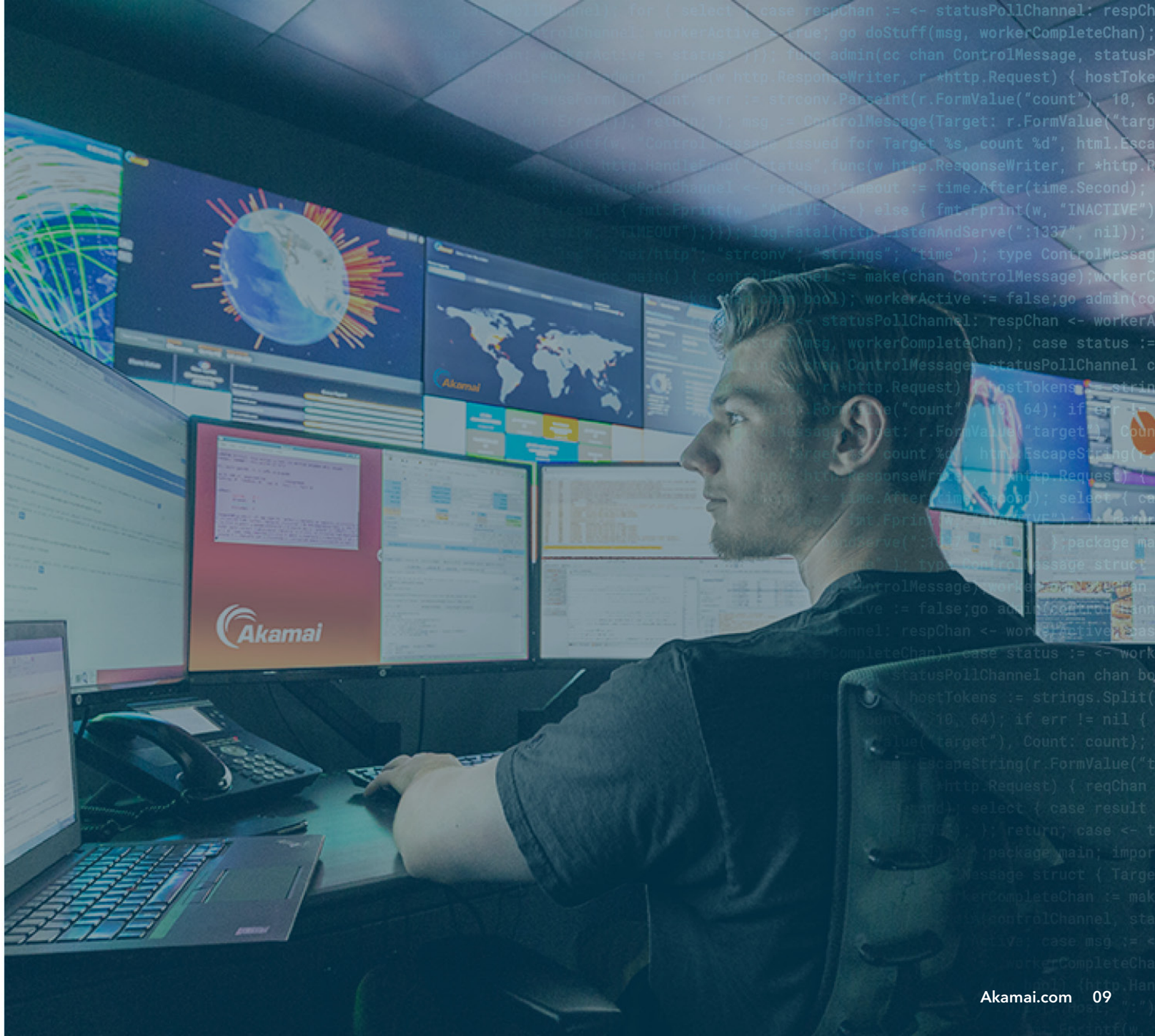
最後，業界許多知名雲端型 DDoS 緩解服務供應商也僅提供標準的攻擊前、攻擊中與攻擊後的輔助，沒有全天候營運的 SOC (全球安全營運中心) 隨時提供支援。即使有，也伴隨著高昂價格，常會比頂尖供應商專門打造的 DDoS 緩解解決方案還貴。在全面管理的 DDoS 防護解決方案中，服務供應商即成為企業事件應變團隊的延伸，提供專業知識，能迅速應對 DDoS 事件。

在現今這種威脅環境裡，現代的企業顯然需要一個 DDoS 緩解合作夥伴，能在混合環境中支援精簡化安全體驗，同時又能降低攻擊面複雜性。

**DDoS 緩解合作夥伴應成為雲端策略的助力而非阻礙，以協助減輕安全壓力。**

# 特別設計的 DDoS 緩解功能

除了需要端對端的雲端策略，企業也必須考慮端對端的 DDoS 防護。Akamai 採取全方位的方法形成第一道防線，以專屬的邊緣、分散式 DNS 和雲端緩解策略提供保護，且其設計可防止附帶損害和單一故障點。相較於其他雲端安全供應商號稱「全功能」的架構，Akamai 特別設計的 DDoS 雲端可提供更強的恢復力，專屬的淨化容量，以及更高的緩解品質，並針對網路應用程式或網際網路服務的實際需求進行微調。



**Akamai 的 DDoS 緩解解決方案設計旨在雲端直接阻止 DDoS，防止攻擊到達應用程式、資料中心和基礎架構。**

### 邊緣防禦

Akamai Edge (CDN) 利用 HTTP 和 HTTPS 通訊協定遞送並加速網站流量。每個 Akamai 邊緣伺服器均以反向 Proxy 的方式運作，轉送連接埠 80 和 443 的正當 HTTP/S 流量，並在網路邊緣捨棄其他所有流量。這表示 Akamai 每一位客戶均獲得全網路層 DDoS 攻擊即時緩解功能，且直接內建於客戶的網站遞送服務。

### DNS 防禦

同樣技術也適用於 Akamai 的權威 DNS 服務：Edge DNS。此服務可瞬間中斷所有非連接埠 53 的流量。Edge DNS 與其他 DNS 解決方案一大不同之處，在於 Akamai 的設計除效能外，還講究可用性和恢復力以抵禦 DDoS 攻擊，以及多重架構備援，包括名稱伺服器、網路連接點、網路，甚至是分割的 IP Anycast 雲端。

### 雲端流量淨化防禦

Prolexic 是歷經實戰考驗的雲端流量淨化服務，能保護整個資料中心和連線網際網路的基礎架構，防禦所有連接埠和通訊協定的 DDoS 攻擊。將正當與惡意流量均路由至 Prolexic，我們便能建立肯定式和否定式的兩種安全模式，以高準確度主動且即時地緩解 DDoS 攻擊。Akamai 安全營運指揮中心 (SOCC) 的專家即成為客戶事件應變團隊的延伸，在自動化偵測與回應及真人應變之間取得平衡。

# 為何選擇 Akamai

Akamai 擁有全球最大規模且成熟的全球 DDoS 緩解雲端。無論是需要保護個別應用程式、整個資料中心還是權威 DNS，Akamai 的 DDoS 緩解架構均提供最大容量，最高恢復力和最快的緩解速度。

我們已多次成功緩解全球最大規模的 DDoS 攻擊。我們的主動緩解措施可達到真正的零秒緩解，提供業界頂尖的 SLA。我們也能同時為多家客戶提供 DDoS 防護服務，能同時對抗多波 DDoS 攻擊。



Akamai

由於 DDoS 攻擊手法不斷變化，攻擊規模也越來越大，導致供應商必須持續投資、開發並部署各種工具和規則，才能偵測、協調及緩解攻擊。Akamai 致力領先威脅一步，在攻擊開始前即進行緩解。

您的 DDoS 緩解策略應要能夠強化您的雲端策略。Akamai Intelligent Edge Platform 提供 DDoS 防禦強化您的雲端策略，協助客戶將防護功能延伸，涵蓋核心系統、雲端和邊緣，將風險降到最低，同時更保留了雲端策略未來進化的彈性空間。

# 歡迎聯絡我們，瞭解如何保護您的企業

**進一步瞭解**

NetFOS 逸盈科技

DDoS 防護請洽逸盈科技
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 976-8909

*Akamai 為全球最大型企業遞送安全的數位體驗。Akamai Intelligent Edge Platform 涵蓋範圍橫跨企業到雲端，讓客戶及其公司能夠享有高速、智慧與安全的體驗。全球頂尖品牌均仰賴 Akamai 提供靈活解決方案擴充多雲端架構，幫助品牌獲得具競爭力的優勢。Akamai 領先業界，讓決策、應用程式和體驗更貼近使用者需求，並保護他們免受攻擊和威脅。Akamai 的產品組合包括邊緣安全防護、網站與行動效能、企業存取及視訊遞送解決方案，全都享有無與倫比的客戶服務、分析服務以及 24 小時全年無休的監控支援。想瞭解為何世界頂尖品牌均信賴 Akamai，歡迎瀏覽 **www.akamai.com** 或 **blogs.akamai.com**，並在 Twitter 追蹤 **@Akamai**。亦可以在 **www.akamai.com/locations** 找到 Akamai 的全球聯絡資訊。2020 年 11 月發行。*