Arbor Cloud℠

多層式全球雲端 DDoS 安全保護解決方案

企業正竭盡全力保護其全球網路免於遭受今日的複雜 DDoS 攻擊。利用 Arbor 雲端安全解決方案（Arbor Cloud），我們可緊密整合企業內部部署的防禦系統與強大的雲端流量清洗服務，以提供可防禦 DDoS 攻擊的全面安全保護。

可防禦目標型 DDoS 攻擊的多層式安全保護

Arbor Cloud 採用分層式 DDoS 安全防護技術，可針對 DDoS 攻擊提供最佳的威脅防禦實作。企業端安全保護服務可抵擋狀態表耗盡攻擊，以便保護企業內部的安全基礎設施。此外，它有助於防禦可繞過防火牆和入侵防禦系統的偵測並鎖定關鍵業務應用的隱形應用攻擊。同時，由 Arbor DDoS 安全專家所組成的隨需流量清洗服務團隊，可抵禦對企業端傳送超大流量，因此非常難以消除的巨型流量 DDoS 攻擊。

Arbor 在每一個安全保護層提供領先業界的專業知識和技術，旨在分析網路流量、消除 DDoS 攻擊，並且將「乾淨（clean）」的流量轉送到網路中的目的地。

全球最先進的企業端 DDoS 安全保護技術

Arbor 領先市場的 DDoS 安全設備可部署在企業網路中，是企業安全防禦的第一道防線。這套易於部署的設備在設計時納入了可自動偵測、減輕和消除攻擊的功能，因此可在攻擊對關鍵應用或系統造成危害之前將它擋下來。它是專為防禦當今的多層式 DDoS 攻擊而設計的安全設備，可抵擋：

- 應用層攻擊
- 狀態表耗盡攻擊
- 巨大流量攻擊（直到超出網路裝置的限制）

Arbor Cloud 企業端解決方案提供即時的攻擊透視度，並可封鎖主機甚至封包。這套企業端解決方案還提供企業所需的靈活性，讓您能在需要時更改攻擊反制對策與臨界值。它還包括主動告警功能，可通知資安工程師已被擋下來的活躍攻擊，以及其他需要特別留意的網路事件。

強大的隨需式雲端流量清洗功能

發生攻擊時，防禦速度和靈活度是維持企業永續經營的關鍵。一旦偵測到巨型流量攻擊，這套企業端解決方案可當作第一道安全防線，以便將對內傳送的流量重路由至 Arbor 全球四大流量清洗中心的任一個中心，以便進行雲端攻擊消除。發生這種狀況時，Arbor Cloud 24x7 全年無休的安全運作中心（SOC）可與貴公司 IT 團隊共同合作，以便透過預先確定的方法，迅速重導惡意 DDoS 流量，使其遠離貴公司的基礎設施。

Arbor Cloud 提供全球流量清洗能力，可避免當今最大、最複雜的攻擊，對貴公司重要資源和資產的可用性造成威脅。

重要特色與優點

企業端安全保護

提供防禦巨大流量攻擊的第一道防線，可抵擋以微小而緩慢的流量，躲避防火牆和 IPS 的偵測並導致關鍵業務應用停擺的「低慢型」攻擊，並可防範會耗盡現有安全設備資源的狀態表耗盡攻擊（state-exhausting attack）。

雲端安全保護

使用雲端流量清洗（traffic scrubbing）技術，盡快過濾掉有害的巨大流量 DDoS 攻擊。這類攻擊在嘗試阻斷服務存取和業務永續性時，可躲避傳統安全設備的檢查。

協同式安全保護

利用 Arbor Cloud Signaling ™技術來綿密地整合企業內部部署的 Pravail 和雲端保護解決方案，以便加快偵測並且消除攻擊。

由單一廠商提供全球安全保護解決方案

請將貴公司的全球企業網路安全保護任務，交給 Arbor Networks 經驗豐富的安全專家。我們可提供不受網路業者影響的完整安全保護解決方案，包括 ATLAS/ASERT 獨步全球的安全與網路研究與情報技術，以及 Arbor 專家提供的 24 x 7 全年無休的服務與支援。

ARBOR® NETWORKS

Arbor Cloud

Arbor Cloud 提供全球流量清洗能力，可避免當今最大、最複雜的攻擊，對貴公司重要資源和資產的可用性造成威脅。

Arbor 安全工程與回應團隊（ASERT）提供強大的支援

Arbor 安全研究人員擁有可即時檢視全球 70% 的 Internet 流量的能力。這種能夠隨時發現新式威脅的強大能力，使得 Arbor 安全工程與回應團隊（ASERT）能夠開發可及時、自動更新企業端解決方案和 Arbor Cloud SOC 的方法。

ASERT 是 Arbor Cloud 服務的一部分，可透過即將在 ATLAS 入口網站中提供的每週威脅簡報（Threat Brief），為客戶和 Arbor SOC 提供相同的全球威脅情報和洞察力。此外，在出現最新型攻擊或緊急威脅狀況時，ASERT 會立即發佈 Threat Brief，以便通知客戶目前出現的所有威脅。客戶可以在入口網站中看到下列訊息（包括 Threat Brief）：

- **全球威脅地圖（Global Threat Map）：** 可即時透視正在全球各地蔓延的威脅
- **威脅簡報（Threat Briefs）**可針對過去 24 小時發生的最重大安全事件提供摘要說明
- **最重大的威脅來源：**您可從各個面向來查看發動攻擊的來源與活動
- **威脅指數（Threat Index）**可針對惡意的 Internet 活動提供摘要說明與各項詳細的威脅比率
- **最重大的 Internet 攻擊**針對全球各地被用來發動攻擊之最普遍的安全漏洞，提供 24 小時快照

運作方式

Arbor Cloud 使用 Arbor Pravail 解決方案中獨特的 Cloud Signaling ™技術，來緊密整合我們的企業端和雲端安全保護解決方案。

當攻擊塞爆連線頻寬，Arbor Cloud 會開始執行以下的步驟：

1. 當 Arbor 企業端解決方案偵測到攻擊時，它會透過我們獨有的 Cloud Signaling 技術，對 Arbor Cloud 流量清洗中心發出警報。您可預設企業端解決方案，以便在達到所設的臨界值時自動發送警報到雲端，或者也可手動對雲端部署發出攻擊警報。

2. 由 Arbor 備受業界肯定和信賴的 ASERT 研究團隊所支援的 Arbor Cloud SOC（位於美國維吉尼亞州 Sterling 市）可及時通知貴公司所偵測到的攻擊。

3. Arbor Cloud 可根據預先設定的重路由選項，將流量重導向到全球四個流量清洗中心之一：

   - 美國東岸（維吉尼亞州 Ashburn 市）
   - 美國西岸（加州 San Jose 市）
   - 中歐（荷蘭阿姆斯特丹）
   - 亞洲（新加坡）

4. 「清洗」過的攻擊流量將變成合法或「乾淨」的流量，並且開始進行轉送，如此可顯著減少停機時間並將網路可用性最佳化。

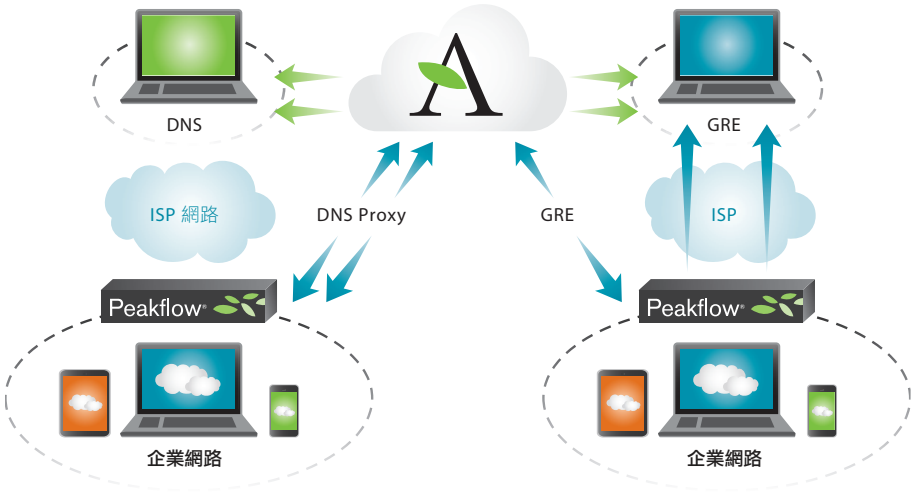
5. 在消除攻擊之後，Arbor Cloud 會將流量重新路由回貴公司的企業網路，並對整體攻擊情況提供完整而詳細的報告。為了讓您深入了解整體作業並獲得所有資訊，Arbor SOC 工程師會在跟貴公司開會時提供這份報告。

靈活的攻擊流量重路由選項

每個網路都是獨一無二的，因此 Arbor Cloud 會在出現攻擊事件時，提供靈活的流量重導向選擇。

DNS 重導向

DNS 重導向功能提供最簡單的流量重導向方法。如果所需保護的主機或 IP 位址數量較少，這是最好的方法。一旦發現攻擊，貴公司可以簡單地將任何受威脅主機的 DNS A 記錄，切換到您指派的 Arbor Cloud IP。接著貴公司的企業網站流量會流經 Arbor Cloud 流量清洗中心，以便過濾掉攻擊流量，並將其餘的流量傳送到貴公司的企業基礎設施中。在攻擊完全消除後，DNS A 記錄會再度被切換回貴公司的企業主機。



BGP 路由

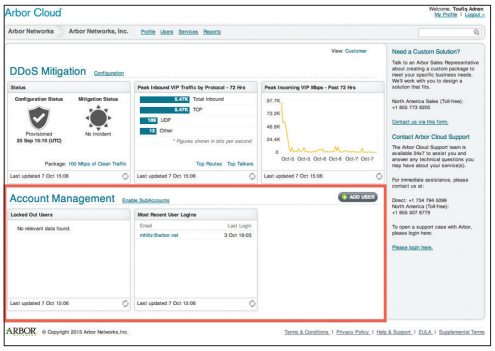
如果您的基礎設施較為複雜，邊界閘道器協定（BGP）路由功能可用智慧轉送方式將流量重導至 Arbor Cloud 流量清洗中心。在偵測到 DDoS 攻擊時：

- Arbor Cloud SOC 安全專家會與您密切合作以便重導貴公司的流量
- 如果 /24 字首受到感染，則取消您的路由器的 BGP 宣告
- Arbor Cloud SOC 團隊會針對受到感染的字首，啟動 BGP 宣告
- Arbor Cloud 流量清洗中心可在幾分鐘內開始防禦攻擊，而 SOC 團隊則繼續監視整個安全保護作業
- 最後，透過 GRE 隧道將「乾淨」的流量轉送到貴公司的網路基礎設施中

當攻擊已經被擊退之後，Arbor Cloud SOC 專員和工程師將協助您針對內部路由器中所有受感染的字首重新建立 BGP 宣告。

透視度和控制性：

Arbor Cloud Portal 提供簡單易用的網頁式圖形操作介面（GUI），讓您隨時存取記帳資訊、攻擊參數、報告和 Arbor Cloud SOC。不同於其他的託管服務，Arbor Cloud 可以讓貴公司能自行控制企業端安全設備，即使這些設備目前正遭受攻擊也沒問題。在攻擊肆虐之際，您可透過 Arbor Cloud Portal 來查看所有的流量統計資料。在攻擊消散之後，Arbor Cloud SOC 專員和工程師會在與您進行面對面會議時，提供詳細而精密的報告。



您可將 Arbor Cloud 當作貴公司的全球安全保護前哨站，讓業界最值得信賴的 DDoS 產品和最有經驗的安全專家做您的後盾，以便高枕無憂地確保網路和關鍵資源的可用性。

DNS 重導向秘訣

將 DNS 時間設成 Live Low

藉由設定較低的 DNS 存活時間（TTL），您可以更快改變整體 Internet 中的 DNS。TTL 可決定遞迴伺服器快取您的記錄的時間。DNS TTL 越低，這些伺服器從授權 DNS 伺服器中找到新答案的速度就越快。DNS TTL 一般都預設為 86,400 秒（24 小時），在遭受 DDoS 攻擊時這樣的時間太長了。

Arbor 建議您將 DNS A record TTL 設成 300 秒（5 分鐘）。設定變更會立即生效，以協助您重導並保護您的網站流量。

BGP 重導向秘訣

如欲使用我們的 BGP 重導向服務，您必須：

- 最少有 /24 字首（Class C 子網段）
- 支援 BGP（邊界閘道器協定）和 GRE（一般路由封裝）的路由器
- 可終結位於您須防禦之字首外部 GRE 隧道的 IP 位址空間

Arbor 雲端安全保護套裝服務選項

套裝服務選項

- 依據乾淨流量收費的透明訂價模式
- 攻擊消除 = 72 小時使用量
- 標準配置不收設定費
- 除非另行註明，所有費用均採月費制

靈活的服務套件

基於乾淨流量的服務選項：	包含：
• 100 Mbps • 500 Mbps • 1 Gbps • 2 Gbps • 4 Gbps • 8 Gbps • 10 Gbps	• 每年提供 12 次攻擊消除服務 • BGP： 以一個回返（GRE）位置保護 1/24 • DNS： 可保護 5 個主機名稱 • 雲端信令告警與監視 • ASERT 威脅報告、攻擊分析以及警報 • 24x7 的第一級、第二級和第三級支援服務 • Arbor 的「即時威脅消除」服務水準合約

其他選項包括

DNS 選項	BGP 選項
• 額外的主機 • SSL 憑證（每一憑證） • 緊急事件設定 / 改變（限一次）	• 額外的 GRE 隧道端點 • 額外的受保護 /24

企業總部
76 Blanchard Road
Burlington, MA 01803 USA
免付費專線：+1 866 212 7267（美國）
電話： +1 781 362 4300

歐洲
電話：+44 207 127 8147

亞太地區
電話：+65 68096226

台灣
電話：+886 2 2656 7573

www.arbornetworks.com

DS/packetloop/en/1013-LETTER

與 Arbor Networks 緊密相連

Arbor Networks Inc. 協助全球最大型企業和網路服務供應商抵禦 DDoS 和先進網路威脅。根據知名市場調查公司 Infonetics Research，在全球企業、電信業者和行動市場中，Arbor 是 DDoS 安全防禦解決方案的領導廠商。Arbor 先進的威脅抵禦解決方案結合封包擷取與 NetFlow 技術，因此可提供完整的網路可見度，以協助客戶快速偵測並消除惡意軟體和惡意的內部人士。此外，Arbor 還提供領先市場的分析工具，以便動態回應意外事件、進行歷史資料分析，並提供視覺化圖示和訴訟證據。Arbor 努力扮演「知識倍增器」的角色，讓網路與安全團隊都能變成這方面的專家。我們的目標是提供最豐富的網路態勢資訊以及完整的安全上下文（context）內容，因此客戶可以更快解決問題，進而減輕企業可能承受的風險。欲獲得更多有關 Arbor 產品和服務的資訊，請瀏覽本公司網站：arbornetworks.com。您可在 ATLAS 威脅入口網站中找到 Arbor 的研究、分析和洞察解決方案的資訊，以及 ATLAS 全球威脅智慧系統提供的資料。

台北：(02)6600-0123#8888
新竹：(03)666-9001#111
台中：(04)2328-4776#12
高雄：(07)390-0257#106