ARBOR NETWORKS
The Security Division of NETSCOUT

所向無敵的
分散式阻斷服務防護

無與倫比的執行效果、超乎想像的輕鬆負擔
中小企業超強解決方案

現在該是正視網路犯罪的時候了

儘管是媒體關注的攻擊目標，但不僅大企業及政府淪為網路犯罪的受害者，中小企業(SME)也是被攻擊的目標，因為他們受到的攻擊威脅日益嚴重。

蓬勃發展的小型企業其不斷的創新及專業技能，往往是中大型企業的合作目標，但大多數小型企業並不如大企業般有足夠的人力、財力、物力來保護公司重要資源，網路攻擊者也深知這一點。因此網路駭客常常想透過小型企業作跳板，攻擊他們中上游的合作伙伴，以便獲取更有價值的資料。

另外，對網路應用及服務愈加依賴，例如對客戶或是合作夥伴的入口網站，也增加了分散式阻斷服務(Distributed Denial of Service，簡稱DDoS)攻擊的風險 (及潛在成本)，尤其是現在要發動此類攻擊的成本及技術複雜度非常低，因此現在此類攻擊背後的動機比以前更多樣- 包含勒索企圖、對公司作為的抗議，甚至是不滿的客戶或是離職的員工之報復行為。

現在只要一點的技術跟錢，任何心懷不滿的人都可以發動攻擊-- 很可能阻斷一個企業的成長，甚至在最糟的狀況，讓他們關門大吉。

小型企業的網路安全問題因為歐洲對保護客戶資料的新規範而變得更為迫切，歐盟新的一般資料保護規範(General Data Protection Regulation)將於2018年生效，它可能因安全漏洞造成客戶資料洩漏，而使公司被罰款兩千萬歐元，或是罰到4%的年營業額，且以金額較高者為主。

中小企業需要所向無敵的DDoS防護，因為您不能一直依賴您的網路服務提供業者(ISP)來保護您。

「三分之二的小型公司已在過去兩年間成為網路犯罪的犧牲者。」
小企業聯盟[1] (Federation of Small Businesses)

[1]「網路順應力：在數位經濟下如何保護小型企業」(Cyber Resilience: How to protect small firms in the digital economy)，小企業聯盟(Federation of Small Businesses)，2016年六月

用輕鬆且可負擔方式來保護您的企業

來自Arbor Networks®的Availability Protection System (APS)是一個就地部署(on-premise)的安全解決方案，它專注於保護網路邊界(network perimeter)以保障商業系統及服務的連續性及可用性，避免其遭受快速氾濫的DDoS攻擊及其他先進的威脅(advanced threats)。

原本是為了大型企業嚴格的安全需求而開發，Arbor為它的APS 2600設備增加了一個100M的授權選擇，所以小型及中型企業也可以享有高等級的就地部署防護，但是只需更輕鬆負擔的價格及使用更容易部署的平台。

它納入了精密的攻擊偵測及緩解(detection and mitigation)科技，不但提供完整的網路活動視野，也能快速啟動補救措施，並做出專業的完整阻隔，因此它能在攻擊影響重要應用及服務之前，將其化解。

藉由雲端傳訊(Cloud Signaling)與雲端的DDoS服務連結，它也有能力將您的防護向前推向更遠；所以它能在大量攻擊威脅到可用性時，自動警告上游的服務提供業者，如您的ISP或Arbor Cloud，以確保攻擊很快地被緩解。

五個選擇APS 2600的理由

1) 負擔輕鬆
許多針對中小企業的DDoS防護產品，要不然是其他產品的附加產品，要不然就是缺乏重要的功能性，以壓低售價。

但使用APS 2600的話，您依然可以享有與企業級產品同等級的安全保障，100M版本現時只需$17,995起，因此現在您得以輕鬆地部署您長久企盼，也是您公司真正需要的解決方案。

2) 簡單
如果您的技術專業還不足，APS 2600就是您理想的選擇，因為任何人都可以部署它；它的「即插即用」(plug & play)設計，意味著您可以使用預設的設定做快速又容易的安裝。

因此您幾乎可以馬上開始保護您的企業組織- 即使它正遭受攻擊；長遠而言，您還是可以輕易做出調整，以符合貴公司特定的需求。

其簡易的設計及使用者介面早已贏得業界的肯定，包含2016年由資訊安全產品指南(Info Security Products Guide) 所頒發的「最佳安全防護硬體」 (Best Security Hardware)金獎。

「Arbor APS能在最少的設定下，甚至是在攻擊發生時，完成部署，提供立即可用且經過驗證的攻擊辨識及緩解能力。」
2016年資訊安全產品指南獎

3) 有效
雖然兼具便宜及可用性，但APS 2600還是納入了企業級的工具組，在其影響您的網路及服務可用性之前，就阻擋TCP狀態耗盡(TCP state-exhaustion)及應用層的攻擊，所以您得以從與全球大型企業同等級的保護中獲益，因為此產品本來就是針對他們而開發的。

特別是它從Arbor的ATLAS情報饋送(Intelligence Feed)功能中不斷獲取最新的威脅情資，當新的攻擊資訊被發現後，該資訊就會被自動地傳送到所有Arbor的產品上，讓它們馬上具有對付新威脅的情報，在貴公司遭受危及之前，就阻擋及緩解最新型態的攻擊或先進威脅。

沒有其他解決方案做到！

五個選擇APS 2600的理由

4) 可擴展性
APS 2600的中小企業版本是我們最小的設備，但是它還是具有高達100 Mbps的就地檢查處理能量。

然而每月只要輕鬆負擔月租費用，它還能無縫地與Arbor的雲端DDoS服務結合，自動及快速的防範無法就地緩解的巨大DDoS流量攻擊(volumetric Attack)，從而讓您的應用及服務不被打斷。

這能避免您的就地防禦被徹底瓦解，讓您能處理任何規模的攻擊，您也不必因此要等待您的資安廠商以手動的方式，開啟額外的雲端防護。

「使用一個混合解決方案是對付流量及應用層攻擊唯一有效的方法。」
Frost & Sullivan[2]

這個方法反映了行業的最佳實務，要阻擋現今的DDoS及先進威脅，產業分析師建議採取一個完整且多層次的方式，以更快、更智慧的方式偵測、防範及反制攻擊。

5) 完整
瞭解DDoS偵測及DDoS防護解決方案兩者間的差異是很重要的，有一些科技，尤其是那些經常是以防火牆附加產品方式銷售的，只是單單設計用於偵測企業組織是否已成為DDoS攻擊的目標，但是並不提供防護及緩解的能力。

而做為一個全然的對比，Arbor卻提供了一個雲端與就地部署防護完整整合的產品及服務組合，而且不間斷地由全球威脅情報所支援。

在這個產業中，沒有其他公司能提供這樣完整的DDoS防護解決方案，這也說明了為甚麼Arbor是第一名的DDoS防護設備提供廠商，橫跨了電信營運商、企業及行動市場[3]。

藉由提供滿足您全部資料保護需求之完整解決方案，我們承擔對您公司完全的防護責任- 因此您不再需要浪費時間以管理錯綜複雜的關係，責任則變得更為清楚，也絕對不會有互相推諉責任的情事發生。

您也有權使用前所未有的技術專業，Arbor網路安全工程及反應團隊(Arbor Security Engineering & Response Team，簡稱ASERT)是一個隨時專注於監控網路威脅、世界知名的網路安全工程師及研究人員團體，有了ASERT的協助，企業組織旗下已負擔過重的網路安全反應團隊能夠強化他們的專業技能，也同時達成整體網路基礎建設防禦的最佳效果。

現在是起而行的時候了

隨著DDoS攻擊數量及複雜度不斷的提升，貴公司幾乎無可避免地將受到攻擊—而可能對您的獲利能力、客戶關係、企業聲譽及成長展望產生嚴重後果。

APS 2600提供大企業層級的防護，但是只要小公司的價格，您真能承擔不使用它的風險嗎？

[2]「揭露萌芽中的DDoS緩解市場」(Uncover the Burgeoning Market for DDoS Mitigation)，Frost & Sullivan，2014年八月。
[3]「DDoS 防護設備: 半年市場追蹤」(DDoS Prevention Appliances: Biannual Market Tracker)，IHS Infonetics，2016年六月

ARBOR NETWORKS
The Security Division of NETSCOUT

關於ARBOR NETWORKS
Arbor Networks，是NETSCOUT的網路安全分部，協助保護全球大型企業及服務供應商的網路，以避免其遭受DDoS攻擊及先進威脅；根據Infonetics Research 的調研，Arbor Networks是企業、電信營運商及行動市場領域中領先全球的DDoS防護供應商，Arbor Networks Spectrum™先進威脅解決方案(advanced threat solution)，透過封包擷取(packet capture)及NetFlow科技的組合，提供完整的網路可視性，能快速的偵測及緩解攻擊活動、惡意軟體及惡意的內部人員；Arbor努力地希望成為一個「力量倍增器」 (force multiplier)，讓其網路及資安團隊成為專家；我們的目標在於提供網路更豐富的樣貌及更安全的內容，讓我們的客戶能更快地解決其問題，同時降低他們業務上的風險。

想要獲得更多關於Arbor產品及服務的資訊，請拜訪我們的網站: arbornetworks.com或是在Twitter上追蹤我們 @ArborNetworks。