DATA SHEET

A10 Defend Threat Control

必備的主動式 DDoS 攻擊情報

A10 Defend Threat Control 為 A10 Defend 套件的其中一個元件，是抵禦日益複雜且數量不斷增加的 DDoS 威脅的必要強化功能。A10 Defend Threat Control 可建立 DDoS 攻擊情報，提供主動且詳細的 DDoS 武器清單，並提供可採取行動的見解，透過阻止可發動或放大 DDoS 攻擊的惡意 IP 來協助組織遏止攻擊。

DDoS：不斷升級的威脅情勢

不要低估 DDoS 攻擊。攻擊可能還未進入活躍週期，或幾乎未得到充分討論，但其勢頭有增無減。現在，部分由於物聯網裝置的成長，以及維護系統正常運作時間、可用性和品牌聲譽的重要性呈指數級上升，使 DDoS 成為越來越危險的威脅。搶先一步瞭解潛在攻擊，對於維護組織的聲譽並確保不間斷的系統可用性至關重要。

DDoS 攻擊透過許多方式進化，像是採用地毯式轟炸等創新的方法。此外，全球網際網路連線呈指數級成長，也連帶擴大了線上裝置網路，使 DDoS 攻擊的起點數量倍增。

為了全面阻止這些持續演變的 DDoS 威脅，需要正確實作 AI/ML、可擴展性、自動化，以及速率限制之外的先進技術。除此之外，還需要另外兩項 DDoS 防禦能力。首先，需要分層式防禦，以協助減輕資安團隊的壓力、最佳化雲端清理使用、應對 DDoS 攻擊的複雜性和數量，同時降低 TCO。其次，資安團隊需要可採取行動的見解，以應對每個受保護基礎架構的細微差別。如此一來，管理員才可根據趨勢和分析見解調整配置。A10 Defend 是一款全方位 DDoS 防禦套件，可提供深入的分層式防禦，並包含 A10 Defend Threat Control 的可採取行動的見解。

SaaS

相關的產品與服務

Related Products & Services

A10 Defend Mitigator

A10 Defend Detector

A10 Defend Orchestrator

DSIRT

DSIRT 支援

與 A10 交談

A10Networks.com/a10-defend

主動式 DDoS 見解與防禦

A10 提供專門針對 DDoS 威脅的情報，建立 DDoS 攻擊情報平台，結合專有資料的收集、驗證和分析，並整理成可採取行動的防禦工具。情報雖非萬能藥，但隨著 DDoS 攻擊的數量和複雜性不斷增加，其確實能彌補不足之處。

資安團隊可以使用 A10 Defend Threat Control 的自訂封鎖清單來滿足組織的特定需求。傳統情報大多為外包、陳舊、範圍更廣。A10 Defend Threat Control 的 DDoS 特定情報與廠商無關，經過徹底研究、經常更新且更加深入。

因此組織可以利用 A10 Defend Threat Control 的可自訂封鎖清單來滿足其特定需求。這些封鎖清單可以與現有的 DDoS 防禦一起部署，也可以用於提升 DDoS 防禦。A10 Defend Threat Control 的自訂封鎖清單可供多數現有的安全裝置擷取。

與現有其他使用方便但卻存在誤報和漏報問題的工具不同，A10 Defend Threat Control 對攻擊者、受害者、分析、向量、趨勢和其他特性的實際見解有助於建立更強大且全面的安全態勢，專為阻止 DDoS 攻擊而量身打造。

重要優勢

降低

TCO

在混合或雲端 DDoS 解決方案中，可減少雲端的波動次數，或透過部署準確的自訂封鎖清單來保留雲端清理能力。建立可靠的第一層 DDoS 防禦，無需專用硬體或更昂貴的雲端清理服務。管理員徹底瞭解現有的基礎架構後，便能善加利用寶貴的見解。

擴大

DDoS 防禦

A10 Defend Threat Control 可做為獨立的 SaaS 平台運作，無需專用硬體即可建立 DDoS 防禦，其封鎖清單也可供路由器或防火牆等現有安全裝置擷取及使用。客製化且自動化的封鎖清單可做為第一層防禦，能應對擁有創紀錄的強度和新型複雜攻擊向量的現代化攻擊，有效管理這些多向量 DDoS 攻擊的數量和複雜性。

遏止

新興威脅

A10 Defend Threat Control 採用專有的資料收集和驗證方法，以提供準確、可採取行動且智慧的資料，可大幅強化 DDoS 防禦。深入瞭解趨勢、向量，以及攻擊者的攻擊方式和受害者的回應方式，有助於組織開發更全面的 DDoS 防禦方案，以應對已知和未知的 DDoS 威脅。

檢驗 DDoS 威脅情勢

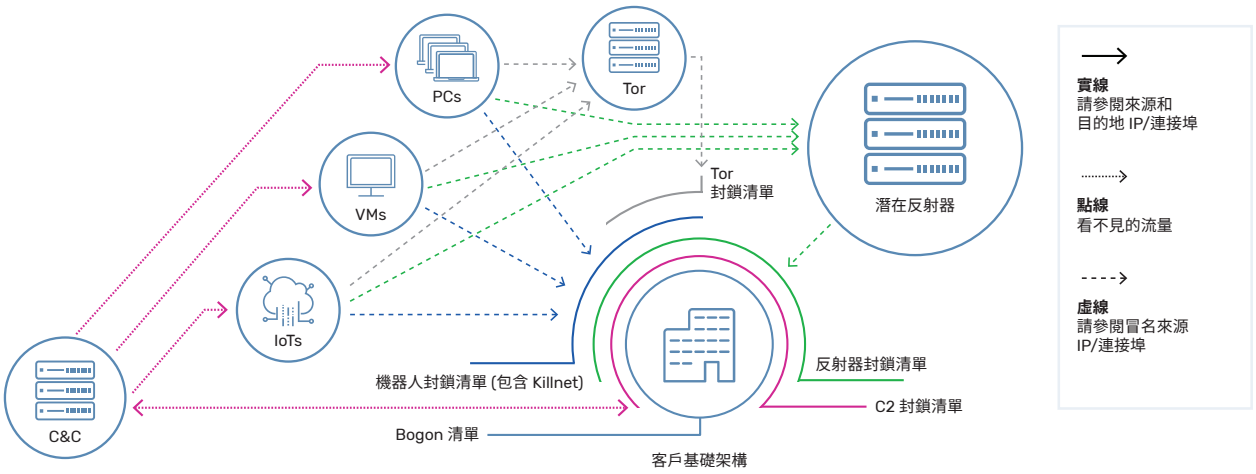

圖 1：不斷擴大的威脅情勢

客戶的基礎架構很容易受到來自多個來源的 DDoS 威脅。惡意軟體可能在 PC、虛擬機器或其他物聯網裝置上運作。命令與控制伺服器是攻擊者管理和編排攻擊的中心樞紐，也是攻擊的真正來源。網際網路上的合法「開放」伺服器可能會透過各種攻擊向量遭到入侵，進而發動反射攻擊。代理伺服器 (例如 Tor) 可以重新定向攻擊，掩蓋來源。

A10 提供三個自訂專有封鎖清單，其零萎縮特性為主要優勢。

- C2 清單：A10 的進階分析可以針對為殭屍網路招募其他系統的受污染系統中的惡意軟體進行逆向工程，藉此確定 C2 伺服器。這份精簡、以 DDoS 為重點的清單提供高可信度，可以阻止攻擊的源頭。此功能對於阻止整個殭屍網路至關重要，試圖在找不到根本原因的情況下阻止個別機器人，就像玩打地鼠遊戲一樣毫無頭緒。
- 機器人清單：A10 的專有資料收集和驗證方法可以分析遭惡意軟體入侵的系統發起的攻擊行為和特性。透過持續分析大量累積資料，A10 Defend Threat Control 可自信地產生清單，識別哪些實體可能是殭屍網路的參與者。
- 反射器清單：反射器是設定放大回應的系統，可產生比原始請求大得多的回應。這些系統在放大攻擊中發揮至關重要的作用，其目標不是用大量請求淹沒目標，而是用少量請求淹沒目標，進而觸發不成比例的大型回應。識別潛在反射器很有幫助，儘管它們目前可能不構成威脅，但其配置和狀態使它們容易受到潛在的利用。

特色

多維度

儀表板

運用即時 DDoS 攻擊地圖和隨附的詳細資料，有助於從攻擊和受害者的角度以視覺化方式呈現世界各地 DDoS 攻擊事件的狀態。使用對數和線性圖呈現長時間的攻擊趨勢，也可以使用進階篩選，並能透過攻擊向量參數 (例如地理位置、持續時間、歷史資料、通訊協定、連接埠等) 進行深入分析。這些見解和發現可下載儲存為 pdf 報告供進一步分析。

思慮周密

受害者識別

DDoS 攻擊不單單透過前兩個或三個攻擊向量執行。我們不斷發現到全新、未曾發現的攻擊向量和方法。A10 Defend Threat Control 可採取行動的見解提供針對反射器、殭屍網路和妥協指標前所未有的可見性。還能根據國家、組織和其他特性，對這些見解進一步分類。其他見解包括對受害者 IP 範圍、受害者 ASN、常見的惡意軟體雜湊、掃描的連接埠、惡意探索的通訊協定、按分類劃分的 DDoS 武器總數等的可見性。這些見解透過攻擊研究/IP 搜尋的形式，以及所包含 IP 的警示和通知，讓管理員能正確設定及準備其基礎架構，進而防範最新且更嚴重的 DDoS 威脅。

彈性

與便利性

做為 SaaS 平台，A10 Defend Threat Control 擁有單一登入、多租戶、通知管理、開放搜尋等便利功能。方便好用的稽核追蹤非常直覺化，可簡化使用者、租戶和工作階段的管理。

資料

永存

A10 專有的資料收集和驗證方法可產生零萎縮資料，這些資料永不過時，始終保持最新狀態。這點很重要，因為攻擊向量持續進化，高風險配置也在不斷變化。如果沒有即時資訊和最新更新資訊，方法可能失去作用。

二元

基線和剖析

A10 Defend Threat Control 呈現攻擊者對您基礎架構的看法，並協助使用者瞭解哪些漏洞可能遭攻擊者惡意探索。透過 IP 位址/網路搜尋時，使用者可以查看 IP 位址/網路是否「遭受攻擊」，或是否正在遭到「武器化」。將報告和建議與這些見解搭配使用可供精細分析。

具影響力

IP 封鎖清單

A10 Defend Threat Control 易於操作，能讓使用者快速輕鬆地部署新的 DDoS 防禦或強化現有的 DDoS 防禦。可以針對殭屍網路、反射器以及命令和控制，產生高可信度和可自訂的 DDoS 特定封鎖清單。開放原始碼封鎖清單也可用於 Killnet 殭屍網路、Tor 代理程式和 IP Bogon。任何現有安全裝置或現有的 SIEM 裝置都可以輕鬆擷取封鎖清單，也可支援特殊使用案例。如果使用者希望整合整個資料集，Defend Mitigator 有能力擷取 9,600 萬個封鎖清單項目。

深入瞭解

關於 A10 Networks

聯絡我們
APAC@a10networks.com

Part Number: A10-DS-15139-TW-01 Mar 2024