DDoS 防禦強化平台：

全面 DDoS 防禦：可見性、防護、報告/建議

透過全面、主動的方法強化或建立 DDoS 防禦

DDoS 做為排名第一的威脅事件，帶動了對專業防禦的需求。現有 DDoS 防護僅依賴硬體或雲端清理，雖然能阻止基本的 DDoS 攻擊，但基本防護是不夠的。現代 DDoS 攻擊的複雜性和數量日益提升，因此我們需要更準確且主動的輔助 DDoS 防禦。面對複雜的基礎架構，能夠輕鬆整合和部署輔助的 DDoS 防禦至關重要。**A10 Defend Threat Control 是一個全面 DDoS 防禦平台，可強化 DDoS 可見性、提供 DDoS 防護並支援主動的 DDoS 威脅調查。**

使用案例 1：

A10 採用專有的 AI 強化型收集和驗證資料方法，使 Defend Threat Control 能提供極度準確的主動和防禦見解。部署 Threat Control 的組織可獲得其網路的對抗視角，或對全球外部威脅進行深入研究。DDoS 攻擊的實施與所使用的向量無關，並可以用鮮為人知的攻擊向量輕鬆執行，從最近的 http2 快速重設漏洞中就能看出。這些見解提供用於調整組織基礎架構的建議，並確保對更多潛在 DDoS 攻擊向量的可見性。

使用案例 2：

A10 Defend Threat Control 可採取行動的封鎖清單使用 A10 的專有探索和驗證方法，確保清單高度準確、可採取行動，並讓現有安全裝置輕鬆摘錄。如此能為目前缺乏 DDoS 防護系統的組織提供第一層的 DDoS 防禦。如果組織已有 DDoS 防護，也能輕鬆新增 Threat Control 的封鎖清單，以更全面調查和防護 DDoS，進而強化現有 DDoS 防護系統的有效性。這些封鎖清單遵循組織專屬的客製化和 ISP 準則，因此可確保清單更加有效，並符合組織的特定需求。此外，也可將這些清單部署到組織的 ISP，在遭遇主動 DDoS 攻擊期間充當額外的防禦層。

A10 Defend Threat Control 優勢

- 輔助現有的 DDoS 防禦，或建立準確的第一層防禦，無需 DDoS 硬體
- 獲得有價值的見解、阻止 DDoS 攻擊並注入主動 DDoS 防禦
- 監控和調查潛在威脅並獲得網路的對抗視角

> *阻斷服務攻擊仍無所不在，多年來一直是最常見的事件。*
>
> — Verizon 2023 年資料外洩調查報告

資料來源：verizon.com/business/resources/Tbc9/reports/2023-data-breach-investigations-report-dbir.pdf

請與我們聯絡以安排解決方案規劃對話

1-888-A10-6363
APAC@a10networks.com

請按讚並追蹤 A10 facebook粉絲專頁

| A10-GR-70361-TW-02 JAN 2024