A10 Defend DDoS 防護：

全方位的企業 DDoS 解決方案

DDoS 仍是排名第一的威脅事件，必須採用多向量分層式防禦方案加以因應。A10 的 DDoS 防護是套裝解決方案，結合偵測、緩解、編排及 DDoS 特定情報，提供準確、可擴充、智慧及主動防禦功能，協助對抗現今複雜的攻擊行動。A10 Defend 專為無縫整合所設計，除了能夠確保最出色的防護效果，也能維持營運效率及維護基礎架構安全，對抗持續增加的 DDoS 威脅。

威脅防護

使用案例 1：威脅防護

A10 的雲端原生威脅防護功能，是以 SaaS 解決方案的形式提供，可在盡量不中斷營運的情況下維護企業安全。其中不需要使用專屬的 DDoS 設備，而是以零萎縮的深入資料和分析協助您強化 DDoS 防禦。A10 的 DDoS 特定情報平台也能產生智慧型封鎖清單，在威脅影響營運之前就主動出擊加以阻止。這類清單可輕鬆與現有的安全基礎架構整合，提供統一及高效的防禦功能，對抗日趨複雜且為數眾多的威脅。

威脅偵測

使用案例 2：威脅偵測

A10 的 DDoS 特定偵測解決方案以流量型方法提供高速及高精度的偵測功能，只要三秒鐘就能識別潛在威脅。如此快速的偵測功能，可協助客戶盡量減少停機時間並維持服務可用性，即使正在遭受攻擊也沒問題。解決方案的彈性成為 DDoS 偵測的穩固基礎，不會中斷現有營運。

威脅緩解

使用案例 3：威脅緩解

A10 的 DDoS 緩解解決方案提供強大即時的防護，對抗流量型及應用層的 DDoS 攻擊，協助確保企業在最有攻擊性的威脅期間持續上線運作。A10 具備自動升級功能，可運用智慧功能遏止損害，無需手動介入。解決方案可內聯部署，或透過 BGP 路由或 DNS 路由進行整合。如果企業遭受預期之外的流量高峰，A10 目前以混合解決方案的方式提供雲端清理功能，可在必要時重新導向流量，確保持續安全性並維持正常運作時間。

A10 Defend DDoS 防護優勢

- **事先掌握威脅：**運用深入、準確及零萎縮的情報，在攻擊中斷業務之前就加以偵測及封鎖。
- **穩定的正常運作時間：**自動、智慧及可擴充的緩解功能，可確保正常運作時間，即使在大規模攻擊期間也沒問題。
- **簡化防禦：**專屬的編排功能可降低複雜度、加快回應時間及提升準確度，以便加速復原。

> *阻斷服務攻擊仍無所不在，成為最主要的事件模式。*
>
> — Verizon 2024 年資料外洩調查報告

資料來源：verizon.com/business/resources/Tfd3/reports/2024-dbir-data-breach-investigations-report.pdf

請與我們聯絡以安排解決方案規劃對話

apac@a10networks.com
A10Networks.com

請按讚並追蹤 A10 facebook粉絲專頁