DELL Technologies

DDoS：採用 Dell Technologies 強化網路安全和復原能力

DDoS 攻擊威脅日益加劇

分散式拒絕服務 (DDoS) 攻擊已然成為數位時代最普遍、最具破壞性的威脅之一。DDoS 攻擊是利用遭入侵裝置所在的廣大網路，用龐大流量對目標系統、伺服器或網路進行洪水攻擊。這種持續的流量暴增會拖慢運作速度，甚至使其完全停擺，這往往也會使進行中的業務癱瘓。

從新創公司到跨國企業，沒有組織能倖免於日益加劇的 DDoS 攻擊夢魘。隨著企業對數位基礎結構的依賴度與日俱增，這些攻擊會帶來從財務損失到聲譽受損等毀滅性後果。Dell Technologies 深知此挑戰的嚴重性，因此提供可擴充的創新解決方案，協助企業強化防禦能力並渡過難關。

什麼是 DDoS 攻擊？

DDoS 攻擊是指攻擊者從多個來源發送龐大流量，意圖癱瘓網路、服務或伺服器的正常運行。攻擊者利用殭屍網路發動攻擊，而殭屍網路則是攻擊者遠端控制的受感染裝置網路。

DDoS 攻擊的運作方式

1. **招募殭屍網路：**網路犯罪分子用惡意軟體感染數千或數百萬部裝置，藉此形成一個殭屍網路，用來動員以發動攻擊，使您的業務無法運作。
2. **流量洪水攻擊：**攻擊者會指示殭屍網路向目標伺服器發送大量要求，導致系統變慢、當機，或讓合法使用者無法使用伺服器。
3. **系統超載：**系統遭到非法流量淹沒，無法執行合法要求，導致服務中斷或嚴重延遲。

常見手法

- **流量式攻擊**，利用龐大流量來耗盡網路頻寬。
- **通訊協定攻擊**，利用 TCP/IP 等通訊協定的漏洞來消耗資源。
- **應用程式層攻擊**，鎖定特定應用程式 (例如網站或資料庫)，中斷其功能運作。

這些攻擊不斷進化，因此對於想保護營運的企業來說，實為一項艱鉅的挑戰。

對企業的影響

財務負面後果

一次 DDoS 攻擊便可能造成數百萬美元的收益損失、停機時間和復原開銷。對於仰賴即時交易的業務 (例如電子商務平台和金融服務)，即使是短短幾分鐘的服務中斷，也會造成嚴重影響。

營運中斷

DDoS 攻擊造成的中斷會降低生產力、使關鍵流程延誤，並阻礙對基本服務的存取。對於醫療保健或製造等行業來說，營運停機時間可能會造成影響深遠的後果。

聲譽受損

當顧客客或戶遭遇服務中斷時，他們的信任感會減弱。長時間或重複發生事件會對組織聲譽造成長期損害，導致客戶流失和市場信心下降。

真實案例

2020 年曾發生一件備受矚目的案例，一家大型金融機構淪為 DDoS 持續攻擊的受害者，導致其線上銀行服務關閉數小時。直接收益損失加上聲譽受損，造成的損失超過 **$5,000 萬美元**。

令人擔憂的統計資料

Zayo Group 的 DDoS Insights Report (DDoS 深入解析報告，2024 年 2 月) 指出，未受保護的組織平均每分鐘花費 **$6,000 美元**，導致 2023 年每次事件的平均成本約為 **$408,000 美元**。此外，此類攻擊的頻率不斷上升，**每年通報的攻擊次數超過 1000 萬次**。這些統計資料突顯出設置健全預防機制的迫切需求。

2,050 萬

2025 年第 1 季阻擋的 DDoS 攻擊次數

資料來源：2024: Cloudflare DDoS Threat Report (2024 年：Cloudflare DDoS 威脅報告)

採用 Dell Technologies 對抗 DDoS 攻擊

Dell Technologies 提供一套先進的解決方案，協助企業預防、偵測 DDoS 事件及從中復原。

透過 Dell Trusted Device 強化端點

端點是指 DDoS 相關威脅的關鍵進入點。Dell Trusted Device 提供內建於硬體的強大安全功能 (例如 Secure BIOS 和 SafeID) 可防範未經授權存取並維護系統完整性。

伺服器安全性

Dell 的伺服器解決方案配備內嵌式安全措施 (例如 Dell Trusted Server 技術)，其中包括：

- **硬體根信任：**此功能可確保在開機階段對伺服器的硬體元件進行驗證，從而提供保障安全的基礎層，防範竄改行為或未經授權的修改。
- **內建安全功能：**Dell 伺服器隨附自我加密磁碟機和端對端開機驗證功能，可防範未經授權的存取，並建立對資料完整性的信心。
- **網路韌性：**此策略包括偵測異常、漏洞及未經授權操作的能力，讓組織能夠從網路事件中快速復原。
- **全方位資料保護：**Dell Trusted Server 解決方案具備整合式安全機制，可保護靜態和傳輸中資料。這包括先進加密技術和自動復原選項，以確保業務連續性。

這些能力可確保伺服器能夠承受流量暴增，同時維持運作穩定性。在遭受攻擊期間，儲存解決方案可保護關鍵資料的可用狀態和完整性，將中斷狀況降至最低。

儲存安全性

Dell Storage 透過各種整合式安全措施及先進技術，將漏洞數減至最少、及早進行偵測威脅，以協助防範 DDoS 攻擊，並確保在攻擊發生時能迅速復原。主要方法包括：

- **主動威脅偵測：**Dell 儲存解決方案運用智慧型監控功能和 AI 導向的異常偵測功能，識別可能表示發生 DDoS 攻擊的異常存取模式。這些工具可提供即時的安全深入解析，並可觸發自動化威脅回應機制，以減輕攻擊造成的影響
- **信任根架構：**此架構內建於儲存控制器中，可確保韌體真實性並防止未經授權的修改，從而強化儲存硬體的安全性，並降低 DDoS 攻擊期間遭到入侵的機會
- **多重要素驗證 (MFA) 和存取控制：**建置 MFA 和角色型存取控制 (RBAC)，協助防止對儲存系統的未經授權存取，也進一步防範與 DDoS 攻擊相關的威脅
- **微切分和網路隔離：**Dell 透過隔離儲存系統並限制工作負載之間的存取，將潛在攻擊媒介減至最小，並在遭到入侵時保護儲存系統免受攻擊者橫向移動影響
- **安全快照和不可變記錄檔：**Dell 的儲存解決方案可提供安全快照和不可變記錄檔，以確保資料完整性，並協助組織從 DDoS 攻擊中快速復原。這些功能有助於進行鑑識分析和事件調查，使 IT 團隊能夠偵測和分析攻擊媒介
- **網路復原存放庫：**Dell PowerMax 和 PowerProtect Cyber Recovery Vault 等解決方案可建立實體隔離備份，這些備份不可變，並受到保護以防範勒索軟體和其他攻擊。這些備份可還原以確保業務連續性，不會有再次感染的風險

藉由整合這些全方位安全功能和技術，Dell Storage 與網路韌性解決方案可有效協助組織防禦 DDoS 攻擊，並維持具復原能力的安全 IT 環境。

透過 CrowdStrike 主動監控

在事態加劇前，即時監控和先進分析對於偵測異常流量模式至關重要。CrowdStrike 與 Dell 生態系統整合，運用行為分析和 AI 深入解析來區分合法活動與攻擊流量，從而啟動迅速的補救措施。

Dell PowerProtect 保障資料完整性

在遭受 DDoS 攻擊時，Dell PowerProtect 可確保關鍵資料處於安全且可存取的狀態。不可變備份能力和隔離復原環境，讓企業能在事件發生後還原系統，並將停機時間縮至最短。

透過 Dell PowerSwitch Networking 和 SmartFabric OS 實現進階網路安全性和微切分

在整個基礎結構中提供進階網路切分、嚴格的存取控制和即時流量分析，以增強對零時差攻擊的防禦。

真實實作狀況

一個全球電子商務平台近期採用 Dell 的 PowerProtect 解決方案，結合主動偵測能力，以抵禦縝密複雜的 DDoS 攻擊。透過隔離關鍵系統和部署緊急復原流程，該企業創記錄的短時間內恢復全面運作，也因此減輕財務損失並維持客戶信任。

多層式安全策略

成功對抗 DDoS 攻擊歸功於分層式適應性防禦。Dell 提倡透過下列策略，讓其技術方案更臻完善：

增強防禦的關鍵步驟

- **零信任架構：**實行「絕不信任，一律驗證」模式，詳細檢查每位使用者和裝置
- **進階加密：**對所有層級的通訊進行加密，以保護在潛在攻擊嘗試期間傳輸的敏感資料。
- **員工訓練：**教育員工識別可疑活動並遵循安全作業程序，以防止不慎違規。
- **定期系統測試：**執行例行評估 (包括滲透測試和負載測試)，以評估系統對高流量的準備狀況。

這些動作結合 Dell Technologies 解決方案，可形成強大的防禦機制來抵禦縝密複雜的威脅。

可強化網路安全的合作關係

Dell Technologies 為了擴展其能力，與 **Microsoft**、**CrowdStrike** 和 **Secureworks** 等業界領導者合作。這些合作關係可提供額外的保護層，將最佳威脅情報和先進偵測法整合至 Dell 的全方位架構之中。

運用 Dell Professional Services

除了技術之外，Dell Professional Services 也為面臨 DDoS 挑戰的企業提供專家指導。從事件回應到量身打造的安全架構諮詢，Dell 團隊可確保組織能夠快速復原並強化未來的防禦機制。

打造具復原能力的未來

Dell Technologies 不只是一家技術供應商，更是致力保護您企業抵禦不斷進化 DDoS 攻擊威脅的合作夥伴。Dell 透過結合尖端技術、深度的合作關係及可據以行動的深入解析，協助企業保護營運、維持客戶信任，並積極追求成長。

現在就朝向復原能力邁出第一步。請聯絡 Dell Technologies，強化您企業抵禦 DDoS 威脅的能力，保障您的未來。

Dell Technologies 讓企業有能力克服 DDoS 網路安全的挑戰，證明安全的根基是在互連世界中成功的關鍵。

請造訪 **Dell.com/SecuritySolutions**，瞭解如何解決當今一些首要網路安全挑戰

深入瞭解
Dell 解決方案

聯絡 Dell Technologies 專家

檢視更多資源

使用 #HashTag 加入對話

DELL Technologies