現代資料中心需要全新的安全性方法

虛擬化、雲端和軟體定義網路 (SDN) 正在改變現代資料中心的範圍與功能。工作負載並非一成不變，而是在多雲端及實體資料中心間持續移動。DevOps 團隊利用持續整合和持續部署 (CICD)，迅速推出新的應用程式和服務，以跟上業務的快速步調。微服務、容器與 API 等新技術正在徹底改變應用程式的設計。

大數據分析與新類型應用程式的資料大量湧入。員工、承包商、商業合作夥伴及客戶必須與資料中心不斷擴充的資源互動。儘管如此可提升資料中心的價值，但另一方面也可能增加資料遭竊的風險。

資料中心團隊現在就必須重新思考因應資安的方法。IT 組織疲於奔命，花費 76% 的心力在防護資料中心[1]。

解決之道就是整合性資安架構，透過業界最佳產品一次解決資料中心的三項關鍵需求。

可視性

透過全面的使用者、裝置、網路、應用程式、工作負載和程序可視性，洞悉一切活動。

有了完整的可視性，您可以更有效地偵測效能瓶頸，並改善容量規劃。讓您更輕鬆找出試圖竊取敏感資料、甚至中斷運作的惡意內部人員。您也可以縮短偵測攻擊和事件後續回應與鑑識的時間。這可協助您決定關鍵系統是否已遭入侵、入侵程度，以及有哪些資訊遭到竊取。

思科®方法讓客戶更深入掌握工作負載和應用程式行為。協助您識別使用者、其連線位置以及存取的主機與應用程式資源。我們讓您以更為輕鬆且迅速地找出難以偵測的威脅，並提供安全性分析，以分析惡意網路活動的網路流量。

分段技術

縮減攻擊面透過一致的安全政策實施、應用程式白名單和微分段技術來防止攻擊者在資料中心內的橫向移動。

分段是藉由限制其透過資料中心從一個資源散佈至另一個資源，來減少遭受攻擊的範圍。對於延遲修補週期的伺服器來說，分段技術是相當重要的工具，可降低適當的修補程式資格完備前以及部署進入生產流程前弱點遭到惡意利用的可能性。對於舊版系統來說，分段技術更是保護資源的關鍵，因為這些系統已經不會再有維護版本或修補程式更新。

許多攻擊專注於透過其應用程式的漏洞、無安全防護的連接埠，或拒絕服務 (DoS) 攻擊來直接存取系統，造成資安上的危害。DoS 攻擊不但會損毀系統，還讓攻擊者得以取得管理員的控制權、安裝惡意程式碼，以進行其入侵行動。若駭客無法存取在資料中心的高價值資產，就可以避免許多攻擊行動，而無需繼續偵測或是系統遭到入侵。

對於許多產業（例如公用事業）而言，進階的持續威脅已是司空見慣。這種攻擊幾乎不可能 100% 完全避免。分段技術是延緩駭客攻擊行動的重要工具，讓安全團隊有時間識別問題、限制暴露風險的範圍，並且採取因應措施。

分段技術對於稽核及法規遵循也扮演重要的角色。基於業界要求（例如支付卡產業資料安全標準 (PCI DSS)）以及法規規定（例如一般資料保護規範 (GDPR) 與健康保險可攜性與責任法案 (HIPAA)），使用分段技術不但可協助降低需要控制項的系統數量，更可限縮稽核的範圍。

思科可提供多層級分段技術。我們可協助您整合原則，並自動化周邊的強制防護，從資料中心網狀架構、主機，甚至是應用程式的程序。

[1] 思科年度網路安全報告

威脅防護

藉由在資料中心策略性部署多層式威脅偵測器**阻止入侵。**這些偵測器可以快速且動態地偵測、封鎖和回應威脅，防止駭客竊取資料或中斷營運。

所有資料中心的共同需求：保護其應用程式和資料，避免遭受與日俱增的複雜威脅和全球性的攻擊。所有組織都面臨遭受攻擊的威脅；許多實際上已遭到入侵，只是並未察覺。

保護當代資料中心是資安團隊必須面臨的挑戰。工作負載持續在實體的資料中心與多重雲端的環境中移動。因此基礎的資安政策也必須以動態方式隨之改變，以便協助政策的即時實施以及隨時隨地按照工作負載進行安全協調。在包含多個客戶的資料中心（例如公共雲環境中），一名客戶可能會嘗試入侵其他的伺服器，以便竊取專利資訊或竄改記錄。

隨著行動和網頁應用程式的使用，提高客戶的忠誠度，但也另開一個入侵途徑，攻擊面因而隨之增加。員工可能不知情地洩露業務，成了資料外洩的幫兇。駭客通常一開始是取得員工驗證憑證的存取權限。他們的做法是以惡意軟體感染端點裝置，或使用網路釣魚攻擊或其他社交工程，誘騙使用者提供其認證。駭客即可藉此取得「授權」，接著存取單一伺服器或資料中心內的所有伺服器，進一步存取更多使用者帳戶，並繼續朝向竊取資料的目標伺服器前進。

您可以降低業務中斷和資料外洩的影響，做法就是部署全面而整合的產品，透過自動化程序合力運作。這個作法可簡化威脅防護、偵測和緩解作業。

思科客戶可以策略地對南北和東西向流量部署威脅偵測器，以迅速偵測、封鎖和回應攻擊，防止駭客竊取資料、甚至中斷運作。我們可以查看應用程式、作業系統、虛擬機器通訊及網路裝置。在此同時，我們可以藉由思科 Talos™，領先業界的威脅情報團隊的支援，偵測到最新、最先進的惡意軟體。

為什麼選擇思科？

思科協助資料中心團隊隨時隨地透過完整的能見度和全面的多層式分段，為工作負載提供持續的防護。我們的解決方案提供整合式的威脅防護功能，讓您的企業更安全，並提高資料中心團隊的工作效率。

如需進一步瞭解思科資料中心的安全功能，請造訪 https://www.cisco.com/go/securedc

C96-740102-00　2018 年 1 月