

卓越雲端運算方案 中信國際電訊CPC

彈性高效雲端服務 助企業掌握當中優勢

在這數碼世代，企業已廣泛利用雲端運算技術，透過網絡提升各種智能裝置的協作效能，並連接不同的應用程式，以提高營運效率。中信國際電訊CPC以「創新不斷」為核心理念，其SmartCLOUD™雲端服務提供多種方案，涵蓋IaaS（基建即服務）、SaaS（軟件即服務）及VAS（增值服務）等，成為企業業務發展的理想夥伴，在眾多雲端服務競爭對手中突圍而出。

雲端技術可解決跨平台運作及軟硬件需求問題，有助企業提升運作效率、降低硬件的資本支出（CAPEX）及其他資源的投入。但若雲端平台出現問題，存放的數據或資料便定有閃失。因此，確保雲端平台的高效和數據的安全，對中信國際電訊CPC來說是重中之重。

中信國際電訊CPC科技、信息科技及安全服務部高級經理鄧志明指出，現時該公司的雲端服務已相當全面及技術先進，例如SmartCLOUD™ BRR虛擬備份、複製和災難復原服務已經支援「秒級」復原點目標（RPO），「企業若出現網絡或伺服器問題，縱使已用坊間一些雲端備份方案，仍可能會損失數以分鐘計的資料與數據，影響業務。」因此，中信國際電訊CPC提供「秒級」的RPO，將數據損失限制在以秒計之內，大大提高資料復原能力。此外，還提供「分鐘級」的復原時間目標（RTO），使企業可快速恢復數據以免妨礙業務運作，客戶更可針對自己需要而自定備份及復原政策，達到高標準之餘也具彈性。

中信國際電訊CPC深明雲端服務的



◎中信國際電訊CPC科技、信息科技及安全服務部高級經理鄧志明

安全性非常重要，一直致力達到行業最佳標準；現時，公司已通過國際雲服務安全標準，成為香港第一家取得「ISO 27017雲服務資訊安全管理標準」的基建即服務供應商。鄧志明解釋，雲服務的高靈活性讓企業能隨時使用所需的雲資源，但由於雲服務接受多種網絡接入方法，並能簡單地由企業自行開通，以及作資源池共享，所以雲端資訊安全的需求變得愈來愈複雜。「ISO 27017的合規要求正為我們定下一個指引和控制措施，使我們的雲端安全規範邁入一個新的里程碑。」

取得ISO 27017標誌著中信國際電訊CPC對雲端的安全威脅和風險管理，以及為客戶的資料和數據作全面保護，均力臻完善，使客戶能免除雲端安全威脅和風險。除了ISO 27017外，中信國際電訊CPC還擁有另外4項認證，包括ISO 9001、14001、20000及27001，持續為客戶提供優質和可信賴的服務。

一站式雲端服務 度身訂造

鄧志明表示，中小企大多認同及需

要雲端服務來提升營運效率，卻未必有充足知識及人手去運作，「我們知道中小企的資源有限，因此提供SmartCLOUD™ Professional Service專業服務協助他們。我們的專業雲端團隊會先了解客戶的真正需求，並設計最適合的雲端服務，還會協助部署及管理，讓企業使用到最新的技術及最合適的方案，企業因而能夠將資源運用於核心業務上。」

中信國際電訊CPC的服務理念是「創新不斷」，鄧志明透露，最近推出了TrueCONNECT™ Hybrid SD-WAN網絡服務，將不同的接入技術，如LTE、寬頻、專用網絡等，經過整合後統一至單一分集路徑，創建混合網絡。TrueCONNECT™ Hybrid更會因應不同類型應用的重要程度，或需要的服務水平，自動選擇最適合的網絡傳送數據，滿足各種雲端應用需要。鄧志明最後強調，「雲運算的發展極需要網絡技術以至資訊安全服務的配合，中小企可多了解ICT服務供應商可以為他們帶來的可能性，從而作出選擇，為業務拓展增加更多優勢」。

卓越資訊安全服務 中信國際電訊CPC

防患於未然 全面資訊安全保企業商譽

繼全球爆發大規模的WannaCry勒索蠕蟲病毒後，又接連有本港企業被黑客入侵，企業損失的已不單止是金錢，更與多年來建立的商譽悠關。中信國際電訊CPC秉持「創新不斷」的核心理念，為客戶提供全面的資訊安全方案，能防患於未然，有效偵測及防止日新月異的資訊安全威脅，確保企業免受攻擊，保障商譽。

黑客入侵企業網絡的手法層出不窮，已由有跡可尋的病毒攻擊進展至防不勝防的零日攻擊（Zero-day attack），能癱瘓企業的業務運作以勒索金錢，更會把數以十萬計客戶資料外洩，令大小企業都面對前所未有的危機。對於中小企而言，礙於其資源有限，更加難有最新的技術及專業團隊去應付瞬息萬變的資訊安全威脅，因此若不幸被黑客看上，輕則損失金錢，重則連多年的業務數據或客戶資料都付之一炬，損失無法估計。

中信國際電訊CPC科技、信息科技及安全服務部高級經理鄧志明表示，與其他資訊科技解決方案如大數據或雲端運算不同，投入在資訊安全的資源未必可明顯地協助企業節省成本及提升效率，因此企業常忽視他的重要性；但若置之不理，一旦發生資訊安全事故，後果則不堪設想。故此企業應未雨綢繆，為其網絡及數據安全作好準備。

提防零日攻擊 資訊安全方案不可少

要有效防止網絡攻擊，進行網絡安



◎中信國際電訊CPC科技、信息科技及安全服務部高級經理鄧志明

全評估（Security Assessment）是邁向成功的第一步。鄧志明解釋，儘管大多數企業會使用如網絡防火牆的安全產品以保護其網絡安全，但保障仍往往顯得不足夠。「所以我們建議企業應先進行網絡安全評估，以得知隱藏的安全漏洞，從而多做一些針對性的安全保障。」

中信國際電訊CPC的TrustCSI™安全管理服務包含「預防、偵測、修正」服務，配以安全信息及事件管理（SIEM）技術、安全運作中心（SOC）及安全專家團隊7x24全天候監察企業安全狀況，並以大數據和人工智能偵察網絡可疑動靜，安全漏洞和威脅自然無所遁形。

鄧志明指，TrustCSI™不止可偵測到現存的黑客及病毒攻擊，連未有特徵、一般防毒軟件也未能分辨到的零日攻擊也可辨認出來，作第一時間的阻隔，使企業免被入侵。「零日攻擊是最難解決的資訊安全難題之一，如同一種全新病毒一樣，要花相當多時間才能找到合適的治療方案，若能防患未然，則可減少許多損失。」

為對抗這些愈來愈多樣化的資訊

安全威脅，中信國際電訊CPC推出利用機器學習技術偵察潛在網絡威脅的TrustCSI™ Secure AI。這個解決方案背後的技術是透過模仿人體免疫系統的自我學習能力自動進行資料探勘，記錄所有用戶和裝置的「使用模式」，從設備所有的數據中作出分析，建構自我的防護免疫系統，實時辨識潛在網絡威脅並迅速自動回應；再加上SIEM技術和SOC的安全專家團隊日以繼夜幫助企業監察網絡安全狀況，及時發現隱藏的漏洞和違規行為，有效應付各類型的網絡攻擊。

除了科技，中信國際電訊CPC亦深明其資訊安全專家團隊應掌握最新的行業知識，才能為客戶提供最合適的方案。「公司會經常為員工提供培訓，提升其技術與知識水平，以及更了解資訊安全的最新情況，也會資助同事去考取與資訊安全及科技有關的認證與專業資格，持續提升服務水平。」

展望將來，鄧志明表示中信國際電訊CPC會繼續與不同的廠商合作，提供最具前瞻性的資訊安全方案，確保企業網絡環境安全，讓他們安心發展及營運業務。