
要有效地保障企業信息安全，必需要配備安全專家、先進軟件和一級設備，才能使企業無後顧之憂。隨著雲運算的普及，黑客網絡攻擊招數日新月異，企業客戶容易成為目標之一，花大量資源購買安全設備硬件進行防護的概念已經不合時宜，並徒添人手作管理及維護。因此，託管式信息安全服務才是現時的大勢所趨。中信國際電訊CPC TrustCSI™就可以為客戶提供一系列託管式信息安全解決方案，為企業提供全面的網絡防護及專業意見，使企業無後顧之憂，盡享雲運算帶來的優勢。

# 中信國際電訊CPC TrustCSI™信息安全管理服務
# 人、才合一 確保不失

## 雲端防護中小企受惠

雲運算服務的興起對中小企來說是一大喜訊，因為他們能受惠於高成本效益，並同時享有大企業級的技術及服務。但礙於資源所限，往往未能兼顧全面的安全問題，以致難以抵抗層出不窮的安全威脅。中信國際電訊CPC顧問及服務交付經理林慕歡表示，有效的網絡安全防護並不是單靠購買大量安全設備便可以達到，還要配合先進技術及富資深經驗的安全專家全天候監控才能萬無一失。中信國際電訊CPC在信息安全方面已有多年經驗，其TrustCSI™信息安全管理服務範圍廣泛，並充分配合其SmartCLOUD™雲端服務的發展，客戶無論是使用其SmartCLOUD™服務，或是利用其TrustCSI™服務來保護網絡安全，均能體現全面的信息安全支援。

現時中信國際電訊CPC TrustCSI™中包括多種服務，如信息評估服務（IAS）、統一威脅管理（UTM）方案、託管式防火牆服務（MFS）、網絡應用程式安全託管服務（MAS）、託管式安全服務（MSS），與及提供全天候安全風險監控服務的安全運作中心（SOC）。企業可以根據業務需要，選擇最適合的方案。

林慕歡建議，企業可先透過信息評估服務（IAS）在其基建及網上應用層面進行滲透性測試，分析是否存在漏洞或安全威脅，中信國際電訊CPC並會為企業提供修正步驟建議以隔絕安全威脅。林慕歡補充，滲透性測試會嘗試以黑客的角度去進行入侵，以及時發現企業網絡設計的漏洞，一切分析及測試均通過認可的專家團隊進行，確保分析的準確性及專業性。

配合評估的結果，企業還可選擇不同的TrustCSI™服務以全面保障其信息安全。最重要的是，TrustCSI™的服務均由其託管式安全服務（MSS）所監控及管理，在預防、偵測及修正上均使用最佳行業慣例（Best Industry Practice），確保企業得到最專業的無間斷保護。

## 專家團隊及先進技術全力支援

TrustCSI™ MSS由中信國際電訊CPC 3個強大並分布亞洲的安全運作中心（Security Operations Centers，SOCs）作支持，所有SOCs均通過ISO9001、ISO14001、ISO20000及ISO27001的認證，確保在服務質素及信息安全和流程方面達到國際標準，並由專家團隊緊密監控，作24×7全天候運作。而專家團隊方面，他們均擁有各種國際性的安全認可資格，當中包括CISA、CISSP以及CompTIA Security+，可為客戶提供最專業的意見及支援。

TrustCSI™能提供專業的信息安全服務，其中一個核心條件是其使用先進的安全信息及事件管理（SIEM）技術，使透過不同的安全設備產生出來的大數據（Big Data），能得以作專業關聯及分析，達致準確地辨認真正的威脅。而中信國際電訊CPC的專家團隊並會為企業提供實時的警報，使有效地在受攻擊前採取即時的修正方案。

林慕歡強調，中信國際電訊CPC TrustCSI™結合專家團隊（People）、專業流程（Process）及先進技術（Technology），全面保護企業信息及網絡安全，助他們化解安全威脅，安心利用雲端優勢發展業務。

林慕歡表示，有效的網絡安全防護並不單靠購買大量安全設備，還要配合先進技術及安全專家監控才萬無一失。

中信國際電訊CPC

**中信國際電訊CPC**
+852 2170 7101
www.citictel-cpc.com