無縫擴展網絡和雲端保護

分散式企業的安全存取服務邊緣方案

在現今瞬息萬變的數碼化商業環境下，企業需要具彈性的IT解決方案來保持競爭力。安全存取服務邊緣方案（Secure Access Service Edge，SASE）利用簡單易用的SD-WAN編排工具，簡化不斷變化的網絡邊緣（從企業總部到分支辦公室、數據中心和雲端)的網絡流量管理。這項全面管理解決方案，簡化並保護基礎設施，同時提升靈活性和可擴展性。企業可以持續營運，提升應用程式能力及體驗，以及確保整個基礎設施具成本效益地為任何用戶隨時隨地提供服務。

全方位的企業郵件安全和雲端備份，實現業務持續營運

電子郵件攻擊是現今緊密互聯的商業環境下，企業最常見的網絡攻擊之一，超過90%的成功網絡攻擊都是通過電子郵件。為了堵塞此漏洞，我們先進的O365備份和電子郵件安全解決方案，提供24x7全天候的管理服務，以安全加固企業的郵件系統。

除了電子郵件外，企業也需要全面保護其他系統，尤其是隨著企業在各項關鍵任務的工作流程中，越來越多採用虛擬化、雲端運算和雲應用，部分重要的數碼資產已經超出企業的實體業務範圍。為了保護這些資產，我們提供全面的備份解決方案，包括現場和異地備份、虛擬機器備份和實體伺服器備份，以保護企業重要的數據及業務彈性。

識別及預測	• 代碼審查服務 • AI資訊安全威脅識別平台 • 漏洞評估服務 • 滲透測試服務 • 資產梳理服務
保護	• 多功能託管式雲備份及災難復原解決方案 (BRR) • 安全存取服務邊緣 (SASE) • 統一威脅管理 (UTM) • 託管式新世代防火牆 (NGFW) • 託管式網站應用程式防火牆 (WAF)
偵測	• 網絡流量分析 • 託管式安全服務 (MSS) • 端點偵測及回應 (EDR) • 用戶和企業行為分析 (UEBA)
回應及復原	• 威脅搜捕服務 • 多功能託管式雲備份及災難復原解決方案 (BRR) • 安全編排及自動化回應 (SOAR) • 安全事件回應 (IR)
SOC即服務 (SOCaaS)	• 3個跨地域SOCs 共同防護威脅 • 先進的雙核心SIEM技術平台實現快速應對 • 具認證的安全專業人員提供7x24在地服務 • ISO27001國際認證的最佳實踐
專業服務及合規	• 信息安全設備遷移服務 • 中國網絡安全法– 網絡安全等級保護2.0合規諮詢服務 • 信息安全設備遷移服務 • 跨境數據合規評估服務

CITIC TELECOM CPC

TrustCSI™ 3.0
雲網神盾

信息安全管理服務

技術賦能 重新定義

識別及預測　保護　偵測　回應與復原

› 服務在地 連接全球的數智通訊服務伙伴

中信國際電訊CPC
W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com
香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606
荷蘭 T: 31 20 567 2000

TSF2401TC

TrustCSI™ 3.0 雲網神盾

TrustCSI™ 3.0 雲網神盾是我們優化的信息安全旗艦解決方案，為您的企業提供最佳保護。方案針對三個關鍵領域，全面檢視及控制信息風險。首先，在現今需求嚴格實踐數據處理的時代，TrustCSI™ 3.0雲網神盾強調合規性(Compliance)以符合最嚴謹的法規要求。其次，此方案易於部署、低前期投入成本、零維護的安全管理服務 (Security)，應對日益複雜的 IT 環境中衍生的威脅。最後，我們利用先進的人工智能，注入創新(Innovation)和智能能力，顯著提升阻截威脅的速度、有效性和效率。

通過 “ReDEFINED SOC4Future” 策略理念，我們為企業安全時代揭開新一章。作為企業值得信賴的TechOps信息安全賦能者，我們不僅在不斷演變的數碼環境中提供保護，我們亦重新定義信息安全的模式。憑藉多年在信息安全行業的深耕和實踐經驗及先進技術，重塑SOC的核心服務能力、強化營運、賦能企業應對日益複雜的信息安全挑戰。

您值得信賴的TechOps信息安全賦能者

致力提升安全服務

技術賦能重新定義

憑藉累積多年信息安全的服務經驗，通過前瞻性的SOC4Future策略，我們將網絡及信息安全由被動式保護轉化為主動式防禦，協助企業輕鬆應對現今瞬息萬變的網絡威脅，減低安全風險。

隨著現代企業加速數碼轉型，他們獲取了新機遇，但亦因攻擊層面擴大而增加風險。同時，網絡威脅日益更加複雜。因此，可靠及全面的網絡安全現今極為重要。

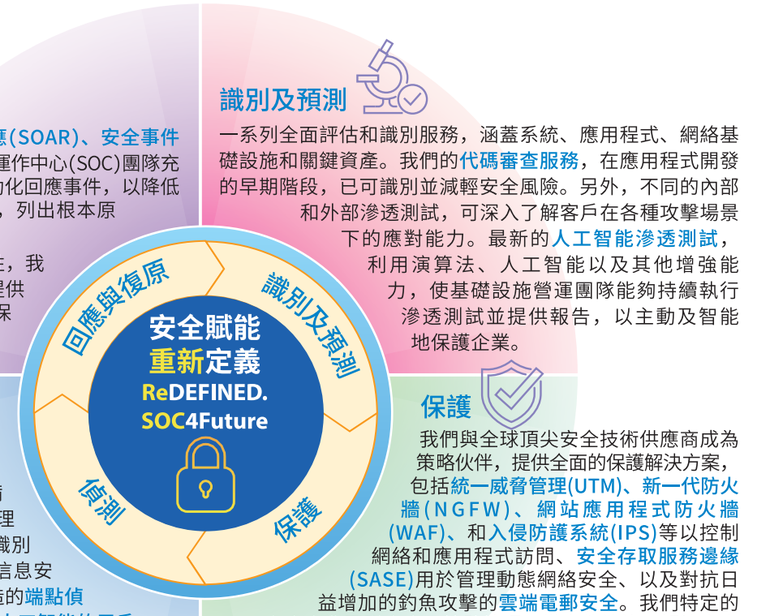
中信國際電訊CPC致力於成為您值得信賴的TechOps信息安全賦能者。我們充分了解不同行業獨特的數碼化信息安全需求，通過SOC4Future策略，賦能世界級TrustCSI™信息安全服務，為企業提供全面保護，有效地識別、預測、保護、偵測、回應及復原各種網絡安全事件，為企業提供全面保護。

憑藉豐富的行業實踐經驗，中信國際電訊CPC的安全專業團隊能協助企業定期開展「AI攻防」實踐，全面評估其IT基礎設施環境與應用的風險，並制定有效的防禦措施，以達到最高的安全保障。此外，我們嶄新的智能安全服務，建基於我們重新定義的網絡安全框架、世界級的基礎設施、屢獲殊榮的專業團隊和前沿技術，能主動地為企業客戶提供無間斷及智能保護，成為企業的「雲網神盾」。

安全賦能 重新定義

憑藉多年來在信息安全行業的深耕和實踐經驗，通過SOC4Future策略，我們為客戶重新定義網絡安全及應對能力，展現五個關鍵要素：智賦網絡安全框架、強化的雙核心安全信息和事件管理(SIEM)平台、積極主動的信息安全策略 –「AI攻防」網絡安全實踐、SOC即服務，以及優化的專業及合規服務，使更全面保障企業安全。

1 創新網絡安全框架



回應與復原

我們創新的安全編排、自動化和回應(SOAR)、安全事件回應(IR)和威脅搜捕服務，賦能安全運作中心(SOC)團隊充分利用威脅情報的能力，協調和自動化回應事件，以降低解決時間，並提供詳細的事後報告，列出根本原因，以支援企業執行未來規劃。

為了進一步加強企業的數碼化靈活性，我們全面的雲備份與災難復原服務，提供彈性的操作模式和複製模型，能確保快速復原和維持業務持續性。

識別及預測

一系列全面評估和識別服務，涵蓋系統、應用程式、網絡基礎設施和關鍵資產。我們的代碼審查服務，在應用程式開發的早期階段，已可識別並減輕安全風險。另外，不同的內部和外部滲透測試，可深入了解客戶在各種攻擊場景下的應對能力。最新的人工智能滲透測試，利用演算法、人工智能以及其他增強能力，使基礎設施營運團隊能夠持續執行滲透測試並提供報告，以主動及智能地保護企業。

偵測

我們位於香港、廣州及上海的三座24x7全天候安全運作中心(SOCs)，備有雙核心安全信息和事件管理(SIEM)平台，為企業快速有效地識別和應對網絡安全事件。我們全面的信息安全服務，包括針對遠端工作環境打造的端點偵測和回應(EDR)解決方案，以及利用人工智能的用戶和企業行為分析(UEBA)偵測異常行為等，賦能企業增強具主動性的綜合防禦能力。

保護

我們與全球頂尖安全技術供應商成為策略伙伴，提供全面的保護解決方案，包括統一威脅管理(UTM)、新一代防火牆(NGFW)、網站應用程式防火牆(WAF)、和入侵防護系統(IPS)等以控制網絡和應用程式訪問、安全存取服務邊緣(SASE)用於管理動態網絡安全、以及對抗日益增加的釣魚攻擊的雲端電郵安全。我們特定的安全專業團隊會全面協助管理，從事件諮詢、解決方案設計和實施、以至配置和日後持續設備管理，確保優化企業的信息安全技術基礎設施並堵塞潛在的安全漏洞，使內部IT員工能夠專注於更具生產力的事項。

2 優化的雙核心SIEM操作模式

我們的區域安全運作中心(SOC)，採用先進的雙核心SIEM技術平台，重新定義威脅情報管理。通過大規模智能數據分析，迅速偵測和回應新興威脅。此創新模式可確保全面的覆蓋範圍並提供可行建議，快速和高效率地滿足不同的信息安全要求。

3 面向未來的SOC即服務

SOC-as-a-Service (SOCaaS)服務體現了未來的智能網絡安全。我們通過基於人工智能驅動的先進安全分析和監控能力，提供出色及優化的安全分析和監控服務。「SOC即服務」(SOC-as-a-Service)由位於香港、廣州和上海的3個頂級自建及管理的7x24安全運作中心(SOC)支持。透過我們擁有國際認證和具合規知識及經驗的專業團隊，提供「服務在地、連接全球」的創新及客製化的安全解決方案，幫助客戶在不斷變化的數碼化環境中，達至數碼安全。

4 擁抱「攻防實踐」協同效應

以積極主動策略，將整個網絡安全循環從被動轉為主動。「AI攻防」實踐涵蓋全棧安全服務，從員工培訓和攻防演練，到網絡保護解決方案、信息安全策略和服務諮詢。攻方執行由AI驅動全方位的評估和模擬測試，而守方則提供縝密的防禦保障，確保全面提升企業對網絡風險的嚴密佈置。

5 優化的專業及合規服務

我們為客戶提供具獨特競爭優勢的「服務在地、連接全球」混合方案模式，無縫融合世界一流的技術知識和設施，以及廣泛的本地業務豐富經驗。另外，我們備有認證的合規專業知識，我們的業務範圍涵蓋從諮詢服務到信息安全設備遷移和跨境數據合規評估。 憑藉全球覆蓋和先進的TechOps能力，賦能客戶高信任度和安全性的數碼化營運。