Tufin Iris 提供雲端一個現代的安全保護方式

解決方案 簡介

多雲環境的自動化安全策略

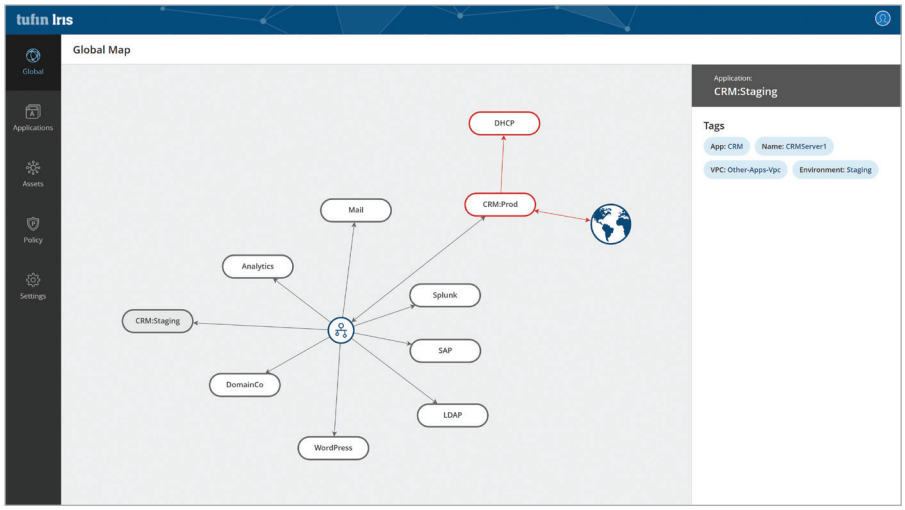
雲端原生平台正在推動數位化轉型，提高業務靈活性並且加速創新。而且，在雲端為先的領域，保護敏感資訊和安全應用程式的需求仍與以往一樣的重要。隨著開發人員使用多個雲端供應商並更頻繁地配置應用程式，這也使得要維護資料的安全變得越來越加困難。為了跟上快速變化的腳步，資訊科技(IT)安全和雲端營運團隊需要全新的，雲端原生的解決方案，以保護關鍵任務的應用程式。老式的安全解決方案均將設計用於保護基礎設備及其虛擬對應架構上。Tufin Iris 整合DevOps pipelines，提供自動化安全性，讓IT 營運團隊能夠重新獲得可見性(visibility)，並在雲端控制其安全策略。

具挑戰性

傳統安全工具基於IP位址和端口位置，以允許或拒絕存取的方式保護應用程式。然而在雲端原生環境中，IP位址是非常短暫的，因此在營運時通常是經由名稱而不是位址以存取資訊。此外，存取控制的策略，乃是結合安全組和身分識別與存取管理(IAM)角色定義之，因此，需要新的解決方案，為IT安全提供可見性，可控性和自動化，以保護業務並確保其合規性。

重獲可見性

單一雲端環境可能已經包含了數百--甚至數千個活動資源。一旦蔓延多個雲端帳戶和供應商，就可能很難知道已經配置了哪些應用程式及其是否都符合安全政策。Tufin Iris 智能地監控雲端，找出所有應用程式並顯示於一張易於導引的地圖之中。這有助於IT安全和雲端營運團隊，快速識別需要立即關注的風險或不合規資源。



重點與優勢

- 獲得對公共雲端安全設定的可見性
- 確保持續性的合規與警示
- 使用安全護欄 降低策略複雜性
- 精密存取控制的微偏析策略
- 無需由代理提交解決方案
- 與 DevOps工具鏈整合
- 登錄即可取得免費帳號: tufin.io

Tufin一覽表

辦公室: 北美, 歐洲,中東與非洲 , 亞太地區

客戶群: 50 個國家中,超過 2,100 家的客戶

領先的行業: 金融, 電信, 能源與公共事業, 保健醫療,零售,教育, 政府機構, 製造業,運輸業

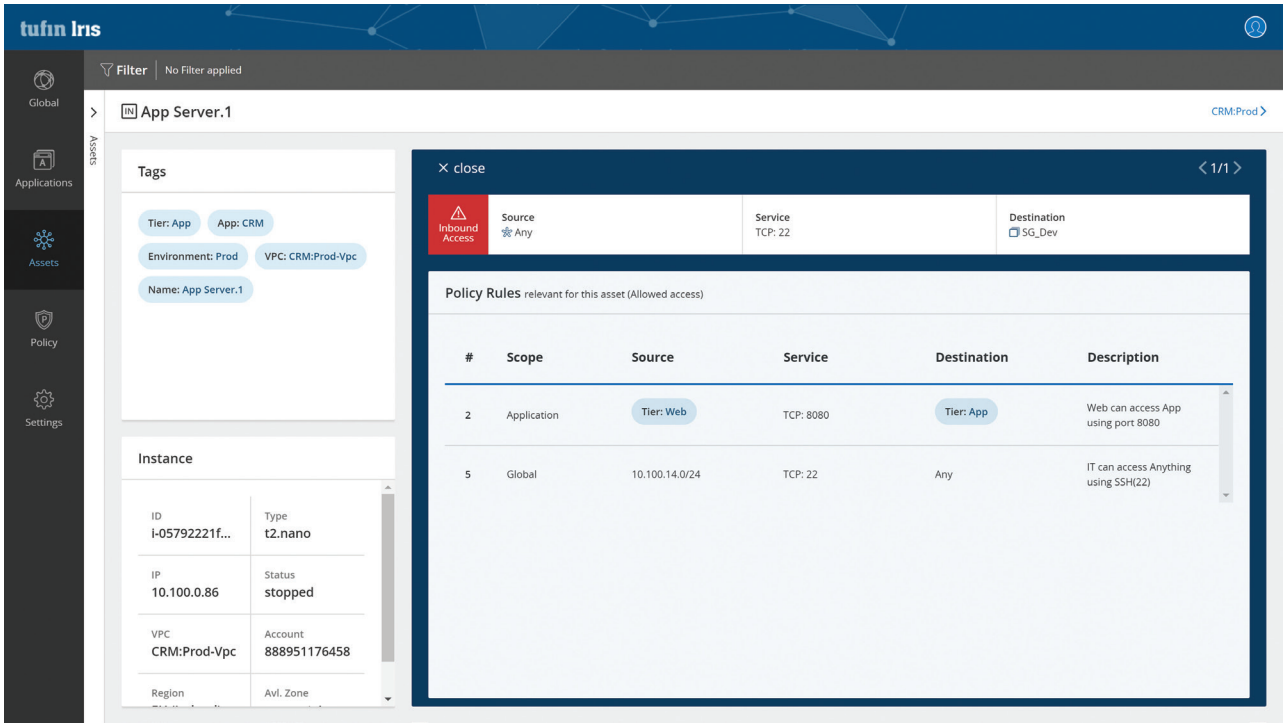
通路夥伴: 全球有超過 150 個積極的夥伴

技術夥伴 & 支援平台:
Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware and more

Azure amazon web services

保持合規性

使用 Tufin Iris，安全團隊可以根據行業、法規或業務要求輕鬆定義其安全策略。在不增加複雜性或導致 “規則膨脹” 的情況下保護應用程式， IT可依合規建立安全護欄，使其適用於全球或應用於一般資源組。例如，護欄可檢查無法從網路存取的儲存數據。關於精密的控制， IT可定義微偏析(microsegmentation)政策，嚴格限制存取以保護關鍵任務資源， 例如限制存取對於處理私人客戶記錄的服務項目。



自動化安全性

雲端的安全防護最好的方式是通過早期預防實現之，通常稱之為 “左移(shift left)” 。且非將安檢安排在最終時做一次性通過的安全政策審查，關於安全政策審查，安全評審整合始於開發週期然後貫穿每個步驟。Tufin Iris的安全策略透過CI / CD工具例如 Jenkins，整合至您DevOps pipeline，可在投入生產之前辨識風險並驗證其合規性。

免費試用

了解 Tufin Iris 如何能幫助您保護您的多雲端工作環境

請上網登錄,取得您的免費帳號: tufin.io

tufin
www.tufin.com

版權所有 © 2019 Tufin
Tufin,統一安全政策, Tufin 架構與 Tufin 標示均為Tufin之註冊商標, 此處提及的所有其他產品名稱均為其各自所有者的商標或註冊商標

SB-01-19

tufin Iris