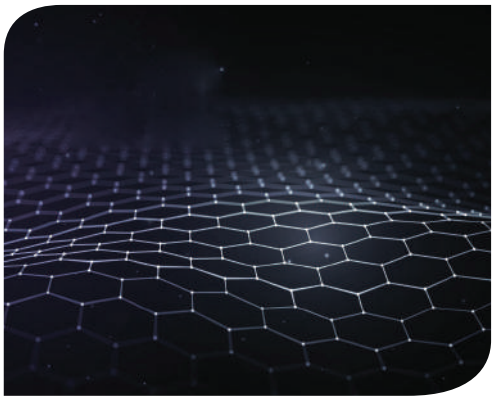


Forescout Continuum Platform

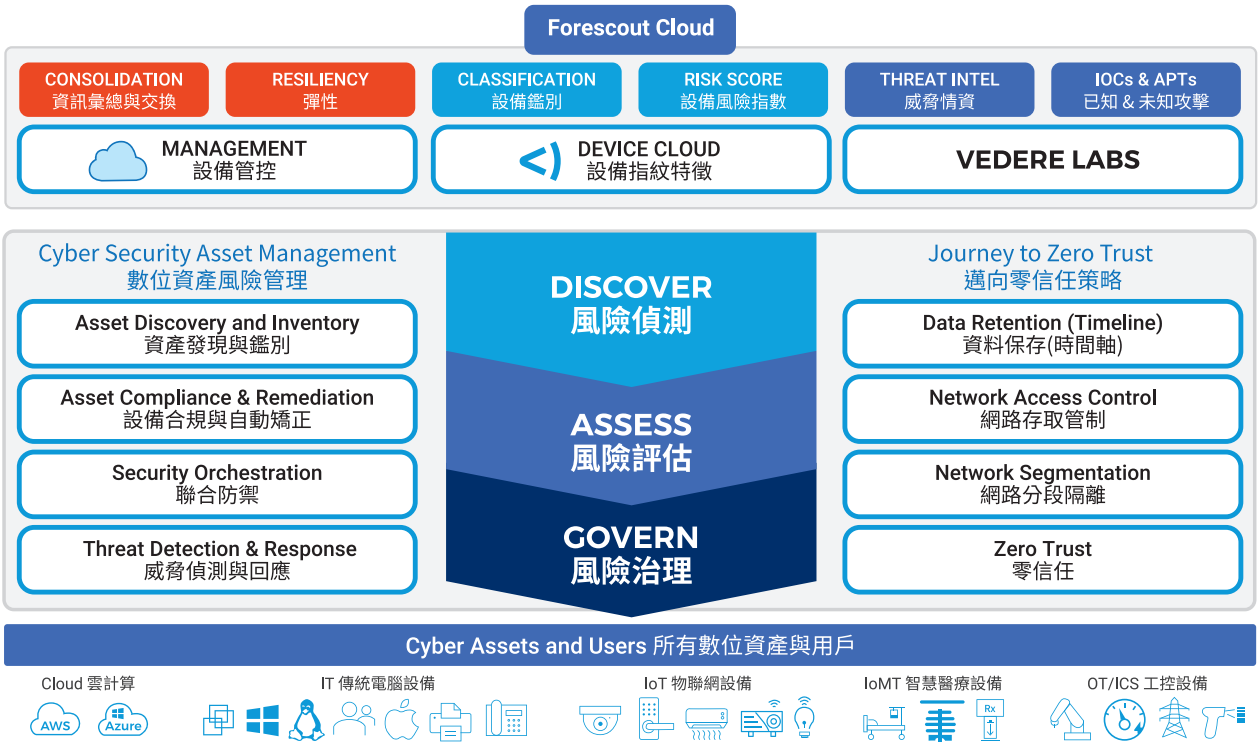
企業需要一個能掌握所有數位資產的資安風險偵測管控平台

全球的資安團隊都面臨著諸多挑戰，其中最棘手的是如何在資安人才短缺的情況下，仍需應對數位資產數量的爆炸式增長。您需要的不是更多資安產品，而是一種“力量倍增器”，一個能夠讓您的團隊提升工作成效並專注於首要任務的平台。從此刻起，Forescout的核心產品，包括 eyeSight、eyeControl eyeInspect、eyeSegment、eyeExtend 及 CyberMDX，將共同納入新的 Forescout Continuum 平台。

Forescout Continuum 平台是網路安全自動化的原動力。Forescout 不僅能夠自動採取網路安全措施，而且只有它能夠針對 IT、IoT、IoMT 和 OT 等各種類型的資產提供所需的可視化和自動化，這些資產共同組成了貴組織的數位化環境。

Forescout Continuum Platform

數位領域資產 (IT-IoT-OT) 資安風險偵測主動防禦管控平台



FORESCOUT
Automated cybersecurity across your digital terrain

Forescout 是一種力量倍增器。它為安全團隊賦予的可視化和自動化能力是無價之寶。

– CISO，佛羅里達州主要醫療中心

使網路實際風險狀況與資安管控政策保持一致

企業的數位化轉型使連線到企業網路的 IT、IoT、IoMT、OT/ICS 等資產呈爆炸式增長。遠端存取、分散式運營和遠距辦公等新型態提高了效率，同時也擴大了網路攻擊面。

每個組織都有自己的一套資安框架：結合最佳實踐、法規要求和企業內部稽核，同時配合資安政策和風險管控實踐，企業目標是使網路實際風險狀況與資安管控政策保持一致。遺憾的是，持續不斷地轉型、升級、新系統上線會使網路實際風險狀況與資安管控政策脫節。這些變化會不斷擴大企業數位化環境的資安風險，並演變為嚴重的營運風險，企業恐需要為此付出高額的成本。

儘管無法預期消彌所有風險，但您可以透過 Forescout Continuum 單一平台使您的網路實際風險狀況與您的資安管控政策保持一致，消除隱匿區與盲點，同時自動化運行達到即時性監控環境變化與矯正持續保持一致性

儘管每個企業的環境都不相同，但要使網路實際風險狀況與資安管控政策保持一致，都依循相同的準則：

資產管理：有哪些資產連線到您的網路系統？ 它們的實體位置和邏輯資訊在哪裡？可視化是一切資安風險管理的基礎—— 您無法保護看不見的資產。

資產合規：能否為資產安裝 Agent？ 如果可以，安裝是否正確？ 配置是否正確？ 登錄的用戶是誰？是否執行了未經授權的應用程式？您必須確認資產處於預期的狀態。

風險合規：資產是否對營運至關重要？ 它是否存在漏洞？ 它的運作狀態是否符合預期？ 如果沒有意識到問題，將無法採取相應的補救措施。

網路分段：資產在通訊方面有何規律？ 它與哪些資產類型通訊？ 通過哪些埠和協定？縱向設備整合能力的網路分段策略能夠縮小攻擊面，同時不會干擾必要的通訊流程。

網路存取控制：是否應該限制或阻斷通訊？主動控制能夠授權訪問存取權限，將使用者和設備分配到各個網段，或者根據設備的安全狀態將其隔離。

自動聯防：我們能夠從其他網路安全解決方案中獲得哪些與資產相關的資訊？ 資產是否安裝適當的修補程式？ 是否存在惡意軟體？ 如果沒有獲得所有可用資訊，就無法作出明確的決策。

管控流程自動化：單一或一連串正確的措施是什麼？ 您希望利用各種資安產品提供的資訊，通過自動化開工單、自動化網路資產監管、自動化漏洞修補等工具來推動正確的措施。

這些步驟在理論上簡單明瞭，但在實踐上卻並非如此。 大多數 IT 團隊無法即時評估所有連線網路的設備，而且無法確認每個設備是否都合規。 此外，很多企業已經購買了幾十種安全工具來管理網路，但是這意味著相關的資訊是片面，欠缺單一事實來源資訊整合可靠的工具。即使能夠識別不合規的設備，但在各種異質網絡和安全基礎架構中應用策略監控和持續合規管控的能力有限。

偵測、評估、治理，三步驟完成數位領域管理全部流程

Forescout Continuum 平台能夠自動發現環境中的所有網路資產並對其進行評估和監管，協助企業安全團隊更加有效地管理數位化資產面臨的風險，使您的網路實際風險狀況與您的資安管控政策持續保持一致

持續偵測及盤點網路中的所有數位資產

Forescout 是唯一能夠持續發現所有網路資產的供應商。他使用 30 多種主動和被動資產發現技術，包括對敏感的 OT/ICS 和 IoMT 資產進行被動深度封包檢測。Forescout Continuum 平台還能夠利用開箱即用的無線、網路交換器和 VPN 設備，發現所有位置和網路中正在進行通訊或未進行通訊的所有數位資產。

通過這些技術收集的數據，可以與 Forescout 設備雲中超過 1500 萬台設備的數據進行參考比對。此外，Forescout Vedere Labs 提供的自動化和大數據技術能夠讓資產分類更加精確。

持續評估網路資產合規性和風險狀況

Forescout Continuum 平台能夠持續發現數位領域中所有網路資產的相關風險，並採取對應的緩解措施。該平台可協助您確保以正確的方式部署、配置和運作安全工具，為您的安全工具投資增值，透過與現有資安解決方案連動，進而達到自動聯防。

借助 Forescout 的自動化設備評估和安全原則執行，不僅能夠實現持續合規的安全運營，還可以輕鬆滿足稽核和報告要求

主動監管網路資產，減小攻擊面，持續降低攻擊行為造成的影響

要想實現出色的監管，不僅需要一系列快速緩解或修補方式，還要能夠根據所有可用情報使用正確的選項。這些選項包括自動化修補、網路存取控制、網路分段、CMDB 更新和跨產品聯防。Forescout Continuum 能夠自動執行回應管控流程，透過Forescout提供的整合模組，結合第三方資安產品實施安全策略。Forescout提供所有網路資產的合規和風險評估結果，並且整合第三方系統的安全分析資訊，快速建立精細化管控政策。

營運中斷可以在短時間內對安全專案造成嚴重的破壞。無論您的整體安全政策是適度還是嚴格，Forescout Continuum 都能夠實施靈活的緩解措施，以保護容易受到攻擊的高風險設備和已被入侵的設備，同時保持重要關鍵型資產正常運作。該平台還能夠模擬策略執行效果並在啟動前監控流量，以便標註可能對網路造成意外後果的資安事件，確保更安全地進行政策變更和最佳化。

成為企業部署零信任的穩固基礎

零信任是一種安全設計方法，而不是可從單一供應商購買到的一項解決方案或技術。無論網路連接是否採用 802.1X，Forescout Continuum 都能夠根據所有網路資產的使用者、設備、連接、狀態和合規情況，自動實施最小特權存取政策，而無需升級或更改基礎架構。

Forescout Continuum 說明企業建置零信任架構的集中式政策管理和政策決策點（PDP），並反映出在不同政策落實點（PEP）之間採取正確措施所需的所有可用資訊。