FORESCOUT

Forescout eyeSight

持續發現、分類和評估設備，以獲得態勢感知和減少風險

CIO正承擔責任，保護日益增加的網路互連系統，尤其是IoT和OT設備。由於您無法保護您看不到的東西，設備數量(和種類)的增加迫使人們需要獲得所有連接實體和虛擬裝置的可視性。這其中包含了由員工、承包商和客戶或者善意的運營人員連接的受管、未受管和未知設備。無論這些設備在網路中的位置(園區、資料中心、私 有雲和公有雲，甚至OT/ICS環境)，它們均需要獲得妥善檢測、配置和說明。

Device Visibility Across the Extend Enterprise

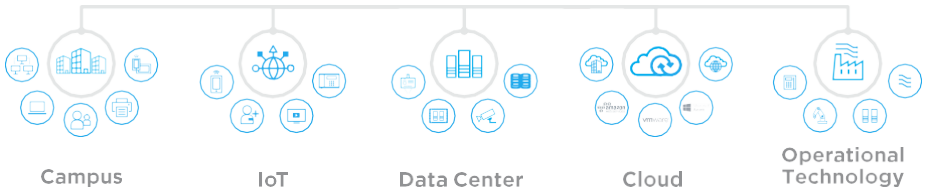


圖1：跨園區、IoT、資料中心雲和運營技術的詳盡可視性。

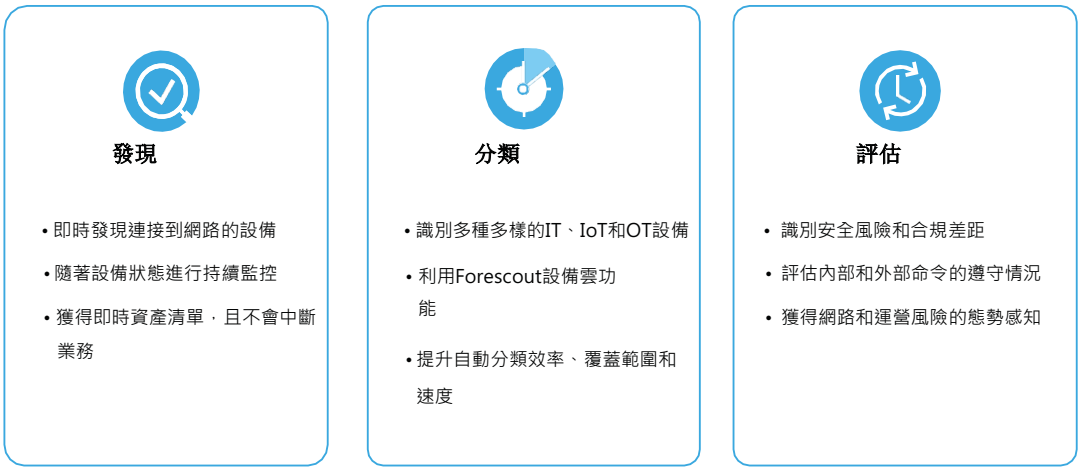
Forescout eyeSight讓您對整個設備情況獲得無與倫比的洞察資訊，而且無需中斷關鍵業務流程。一切始於發現整個企業網路中的所有IP連接設備。但發現只是獲得完全可視性的第一步。為作出正確的策略和控制決策，全面的縱向橫向發現非常重要。發現連接設備後， eyeSight會根據公司策略自動分類和評估這些設備。將發現、分類和評估三種功能有力結合，提供所需的設備完整可視性，從而幫助制定適當的策略，採取適當的措施。

eye Sight

Highlights

- 獲得所有網路連接設備的即時清單，無需安裝代理
- 準確配置設備，以便獲得構建主動安全和合規策略的所需縱向橫向資訊
- 識別非法、存在漏洞或不合規的設備，並創建策略限制風險
- 即時確保安全工具和合規控制正在運行
- 有效衡量和報告合規狀態以及網路風險
- 自動執行常規任務以減少人為錯誤和增加效率

圖2：eyeSight提供的主要可視性功能。



無需安裝代理即可發現及持續監控

IoT和OT設備構成獨特的可視性挑戰。這些設備數量龐大，造成規模挑戰，因為人工發現設備已不再可行。此外，這些設備中，許多無法支援安裝代理程式，並對主動式探測和掃描技術是敏感的，可能造成系統和業務中斷。eyeSight使用20多種主動和被動監測技術(參見圖3)，通過自動發現避免潛在可視性差距：

- 園區網路上的筆記型電腦、平板電腦、智慧手機、BYOD/客戶系統和IoT設備
- 資料中心的虛擬機器、虛擬機器器監視器和物理伺服器
- 公有雲和私有雲上的AWS、Azure和VMware實例
- OT 網路上的醫療、工業和建築自動化設備
- 物理和軟體定義的網路基礎設施，包括交換機、路由器、VPN、無線基地台和控制器

這些發現功能共同減少運營風險，消除可視性盲點，從而在整個擴展企業上獲得完整持續的設備清單。

圖3：主動式和被動式發現技術。

被動式對網路設施及環境	主動式對終端設備	主動式對終端設備
SNMP Traps	Network infrastructure polling	無代理 Windows 檢查 • WMI • RPC • SMB
SPAN traffic	SDN 整合 • Meraki • Cisco ACI	無代理 macOS、Linux 檢查 • SSH
流量分析 • NetFlow • Flexible NetFlow • IPFIX • sFlow	公有/私有雲整合 • VMware • AWS • Azure	NMAP
DHCP request	目錄服務 Query(LDAP)	SNMP queries
HTTP user-agent	網路應用 Query(REST)	HTTP queries
TCP fingerprint	資料庫 Query(SQL)	SecureConnector®
協議解析	eyeExtend Orchestrations	
RADIUS request		

Challenges

- 各自獨立作業的團隊、安全工具和流程導致可視性差距
- 容易出錯的人工流程導致運營和經營風險
- 設備智慧化未到位，使得IT所獲得用於構建防禦策略的上下文資訊過少
- 無法確認已經安裝、配置和妥善運行安全工具
- 無檢測到的非法設備導致不必要的安全和合規風險
- 過時的時間點掃描導致對合規狀態缺乏信心

智慧化自動分類

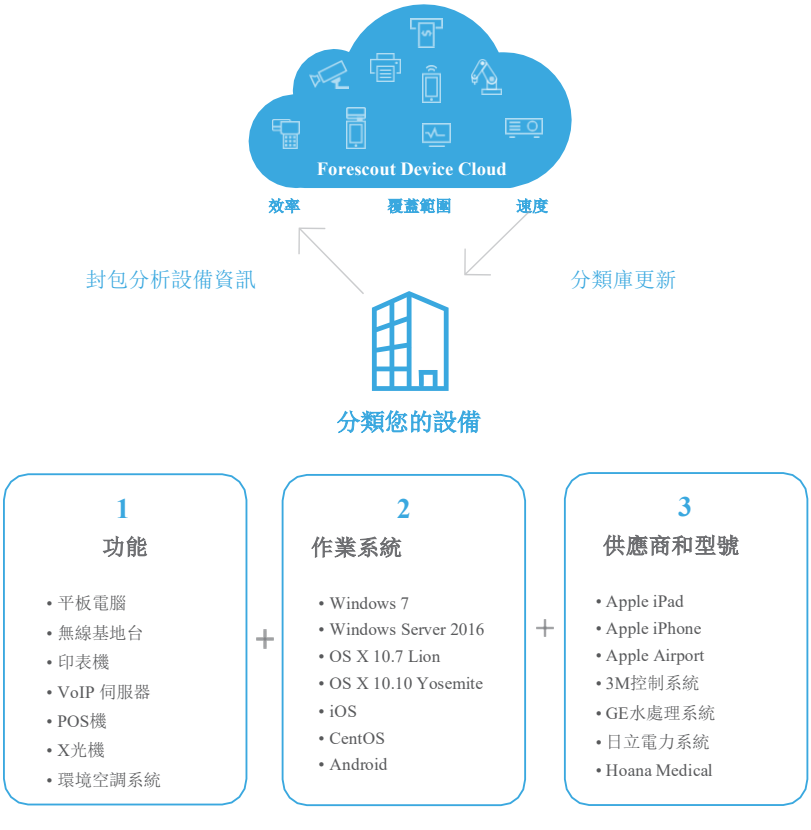
每個設備的完整上下文對創建詳細的策略至關重要。您需要知道每個設備的運行上下文或目的，才能決定如何最好地對其加以保護和管理。設備和多樣性的增加使人工收集上下文幾乎不可能，創建缺乏適當上下文的策略也把運營置於風險之中。eyeSight使用多維分類學來自動分類傳統、IoT和OT設備，以識別設備功能和類型、 作業系統和版本，以及供應商和型號。通過對多達100多種IT和OT協議的深度封包檢測，使 eyeSight能夠對IoT和OT設備獲得深度洞察資訊。

eyeSight自動分類：

- 500多個不同的作業系統版本
- 5,000多個不同的設備供應商和型號
- 來自350多家領先醫療設備供應商的生技醫療設備
- 製造、能源、油氣、公用設施、礦業和其他關鍵基礎設施行業使用的成百上千的工業控制和自動化設備

Forescout Device Cloud為eyeSight自動分類提供支援，確保這一豐富的上下文來源保持與設備增加和多樣性保持同步。Forescout Research利用我們的設備雲*中800多萬真實世界設備的情報，頻繁發佈新概況，改善整個設備場景中的分類效率、覆蓋範圍和速度。

圖4：Forescout設備雲。



截至2018年12月31日

設備狀態評估

設備分類提供有關設備目的的運營上下文，說明設備是什麼。但要獲得完成上下文，需要另一種技術，以便判斷各設備的健康和安全狀況。

eyeSight持續監控網路，評估連接設備的配置、狀態和安全狀態，以確定其風險狀況及是否遵從安全和監管合規政策。

eyeSight 提供關鍵問題解答，包括：

- 是否已安裝安全軟體，是否正常運行，並更新了最新修補Patch？
- 是否存在設備運行未授權應用程式或違反設定標準？
- 設備是否使用預設或較弱的密碼（IoT設備經常面臨此特別風險）？
- 是否檢測到非法設備，包括通過欺騙技術冒充合法設備的設備（以及這些設備是否連接至網路）？
- 您的連接設備中，哪些最容易受到最新威脅攻擊？

設備情報的威力

eyeSight 通過發現、配置、自動分類和評估提供的設備可視性，在Forescout控制台一目了然。您可使用可定制化儀錶板獲得高水準洞察資訊，並在實現風險和合規目標的過程中分享進展快照。這些動態視角可幫助安全團隊：

- 評估特定策略的成功實現程度
- 發生資訊外洩時識別漏洞設備，以加快事件回應
- 追蹤隨時間變化對特定合規要求的遵從性
- 構建風險和合規以及潛在漏洞的可執行和審核視圖
- 深入研究與特定策略、設備類型、位置等相關的故障排除問題區域。

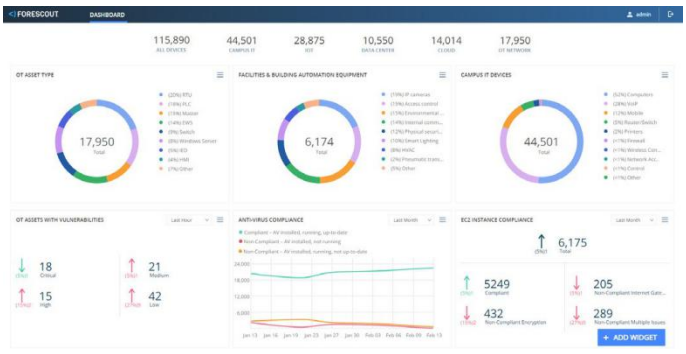


圖5：定制儀錶板，以便為多個業務相關者提供其所需的上下文資訊。

eyeSight 提供的設備可視性還可借助通知操作和API分享給跨職務 IT相關人員。eyeExtend產品組合將設備上下文資訊分享給其他領先的IT和安全產品，以便自動執行工作流程，連動其他系統的回應。

沒有來自eyeSight的關鍵設備上下文資訊，企業可能缺乏信心實施控制策略，因為基於不完整的設備資訊而採定的措施可能讓業務運營面臨風險。eyeSight□提供設計和實施詳細策略所需的深刻洞察資訊，並自動採取有關資產管理、設備合規、網路訪問、網路分段和事件回應的措施。再來，您可以使用Forescout eyeControl和Forescout eyeExtend產品充滿信心地建立基於策略的有效控制以及連動自動化管理。

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

免費電話（美國）：1-866-377-8771
電話（國際）：+1-408-213-3191
支援電話：+1-708-237-6591

訪問Forescout.com，瞭解更多內容

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市前鎮區一心二路128號9樓之1