FORESCOUT

# Forescout eyeControl

## 強制執行和自動實施基於策略的控制，以主動減少攻擊面，快速回應事件

eye Control

IT安全團隊淹沒在大量安全工具報告的日益增加的安全和合規問題中。這些工具不斷產生告警但沒能力採取措施。不幸的是，這些安全工具缺乏足夠縱向設備資訊用以確認安全事件的優先順序，或者缺乏自動化能力執行降低風險的控制措施。結果， 高度熟練的安全團隊浪費大量的時間和人工用來排除低風險問題，無法專注於主動 保護敏感性資料免受外部威脅 降低風險或快速威脅回應。

### 基於策略(Policy)的控制執行

Forescout eyeControl從Forescout eyeSight獲得豐富的縱向設備資訊，讓安全團隊可以 自信地安排優先順序、執行和自動實施基於策略的控制措施。企業可以改善網路安 全狀態，減少攻擊面，加快回應和補救，以快速緩解威脅、安全事件和合規差距。

取決於您的安全舉措，您可以使用 eyeControl 執行網路阻斷和端點修復矯正等措施。 在網路措施方面，eyeControl 可直接整合不同品牌實體和虛擬網路設備-交換機、 無線控制器、VPN、SDN 和 Cloud Base 的網路。端點修復矯正措施可在 Windows、 Mac 和 Linux 端點上無需安裝 Agent 執行，或也可借助超輕量 SecureConnector 執行。

### Highlights

- 保護敏感性資料免受外部威脅
- 防止受感染、有漏洞或非合規設備傳播惡意軟體
- 防止目標攻擊竊取資料或迫使網路中斷
- 幫助確保員工、訪客和客戶對網路的訪問和可用性
- 強制符合內部策略和外部規定
- 自動執行控制措施，以便針對每個情況採取正確措施

圖1.在網路和端點執行策略，隨時間推移增加自動化。


**自信地自動執行控制措施**

eyeControl利用直觀靈活的策略引擎使組織能採用詳細的目標控制。借助易用的動態 範圍(Dynamic Scoping)、布林邏輯(可使用各元件AND、OR、NOT等邏輯運算) 和瀑布策略(階層式)實施精緻的工作流程和綜合措施。策略圖功能便於進行準確的策略創建、策略流程分析，以及在開啟執行措施前微調策略。

安全團隊可人工啟用控制措施，或者為增加安全運營效率，可逐漸引入自動化。從基礎、重複性任務開始，逐漸擴展到更複雜的控制措施，自動化可節省IT技術資源，專注於影響更大的問題。該方法有助於確保儘量減少業務中斷，同時極大改善網路訪問、設備合規、網路分段和事件回應舉措。

> “通常可以自動執行一個端點的操作，需要人工干預時，只需右擊一下。” – *Joseph Cardamone，Haworth高級資訊安全分析師和北美隱私長*

## Challenges

- 網路上的非合規或未授權設備構成較大風險
- 扁平化且未分段網路使組織易於遭 受橫向攻擊威脅
- 無法快速有效回應安全威脅和事件
- 通過安全工具執行持續設備狀態監控的能力有限
- 業務中斷風險限制安全控制自動化

**執行網路訪問**

根據使用者角色（訪客、員工、承包商）、設備分類和安全狀況，控制企業資源的訪問。

- 為訪客和BYOD設備啟用差異化訪問
- 執行網路訪問策略（使用或不使用802.1X認證）
- 採取措施應對網路上的可疑、非法或影子IT設備
- 限制或阻斷受攻擊或惡意設備的網路訪問
- 封鎖或隔離非合規設備，直至解決合規偏差

“我們選擇Forescout平台的一個原因是該技術不依賴802.1X協議，因而極易部署。無需安裝代理，性能更高，更簡便。”
*—Juan Ignacio Gordon，ACCIONA IT安全主管*

**改善設備合規性**

自動執行合規評估，並執行補救控制措施，確保持續符合內部安全性原則、外部標準和行業規定。

- 說明確保妥善配置端點，針對關鍵配置違規（包括較弱的密碼或預設密碼）啟動補救措施
- 確保所需應用和安全代理已經安裝、運行且更新
- 禁用或阻斷可能對網路頻寬或資源生產率造成風險或不必要負擔的未授權應用
- 識別高風險漏洞和遺漏的關鍵 Patch，並啟動補救措施
- 主動鎖定補救措施，例如安裝所需安全軟體、更新代理或應用安全Patch
- 實施策略，自動執行控制措施，以實現雲部署中的配置合規，包括AWS、Azure和VMware®

“藉由 Forescout 解決方案，稽核更快，產生的結果更少，所需修復補救措施更少，我們預計可因此節省數百萬美元。”

*—Phil Bates，猶他州首席資訊安全長*

**實施動態網路分段**

借助通用策略框架，在擴展企業的不同執行技術上應用動態網路分段策略。

- 根據設備屬性、分類和安全狀態動態分配設備至分段組
- 通過VLAN、ACL、WLAN控制和園區和OT網路標記應用分段控制措施
- 通過公有雲和私有雲環境（例如AWS和VMware NSX）中的安全性群組/標籤應用分段控制
- 將非合規和有漏洞設備分段為單獨的區域，尤其是針對僅能在定期維護視窗內修補或補救的設備，這樣可確保業務連續性，同時減少攻擊面
- 根據HIPAA、PCI和SWIFT CSP等規定要求，從網路的其他部分的區域設備和關鍵資料流程執行分段策略

“Forescout不僅可以隔離設備，進行網路分段，還可以發現之前未發現的網路。” *－大型醫療保健組織副首席資訊安全長*

**加快事件回應**

有效地快速遏制威脅和回應安全事件，以儘量減少運營中斷和業務損害。

- 識別尚未遏制或補救的高風險設備
- 識別連接時設備上的受攻擊指示指標（IOC），以減少回應的平均時間（MTTR）
- 快速隔離和遏制受攻擊或惡意設備，以避免惡意軟體的橫向傳播
- 自動執行事件回應，並在受攻擊設備上啟動補救工作流程
- 通過向跨職能事件回應團隊和孤立的技術提供寶貴的設備上 下文(設備連接、位置、分類和安全狀態)，減少MTTR (Mean Time To Repair 平均修復時間)

“Forescout像是擁有一支自動威脅獵人團隊，在我們的全球網路上全天候捕捉威脅。我們現在可以解決之前無法解決的問題。 以前需要幾小時完成的任務現在只需要幾分鐘。”—*Nick Duda，HubSpot首席安全工程師*

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