FORESCOUT
Active Defense for the Enterprise of Things™

# 新世代NAC

無需代理程式、靈活且不中斷的零信任安全，適用於您的企業物聯網。

現今的企業需要一種方法來實施和維護零信任訪問，用於其多種網路類型和多樣聯網設備—園區電腦、訪客設備、遠端辦公筆記型電腦、IoT、OT和智能設備。這些都需要一個現代化網路訪問控制（NAC）平台來完成以下任務:

- 持續識別所有連接的設備
- 評估其安全態勢
- 執行訪問策略
- 自動對不合規或異常行為實施控制

## 零信任說起來容易做起來難

控制所有連接到企業網路的設備很令人頭疼。管理這些系統的IT和安全架構師面臨著以下挑戰:

- 早期的NAC解決方案由於複雜性或對業務運營產生負面影響的風險而失敗
- 企業網路上激增的IoT和OT設備無法通過傳統代理程式進行認證或控制
- 基於802.1X的控制在多品牌網路中不可行
- 排程的網路掃描沒有考慮到偽冒嘗試和其他隨時可能出現的威脅
- 許多零信任訪問替代方案成本太高和或需要太多人力投入

> 曾有人告訴我們可以在一個下午部署好Forescout平台。我看著我的一個團隊成員，我們倆都難以置信。結果我們真的在幾個小時內完成了部署！
>
> **MIKE ROLING**
> 首席資訊安全官，密蘇里州

# Forescout：同業中最佳的新世代NAC解決方案

如果上述挑戰聽起來耳熟，那麼現在就是對Forescout 評估網路訪問控制的絕佳時機。我們可以通過以下方式滿足您的需求並超出您的預期:

### 最全面的可視性

具備20多種主動和被動技術，使連接到您網路的所有設備達到100%可視性，且即時同步。

### 對所有連接設備實施零信任

通過持續的無代理程式監控和統一的策略引擎，控制不合規帶來的影響，可動態隔離和阻斷所有連接到您企業的設備。

### 無中斷部署，為您的網　路提供快速價值

無需代理程式且無需基礎架構升級或802.1X配置，可在數天內獲得全面可視性，並在數週內實現自動化控制。

### 經過驗證的企業級擴展網路

Forescout已累積數以千計滿意的財星1000客戶實績，其中部分已部署200萬個端點，這些客戶證明了Forescout在保護網路安全方面的能力和給予客戶的信心。

### 擴展您的安全和IT投資價值

大多數安全工具僅僅是標記違規行為並提醒您的員工。 Forescout平台包括即插即用的模組，將可視性和控制功能擴展到：

- 與您現有安全和IT管理工具即時共享設備情境
- 協調工作流程並自動化回應操作
- 持續評估安全態勢並執行自動修正設備的合規行為

**“現今的NAC工具最適合幫助隔離設備和未經批准的實體（用戶、區段、設備等），使其無法“接觸”網路。使用這些來自Forescout等供應商的較新的NAC技術， 幫助將未知的和可能未上Patch的設備從您的零信任網路中移除。 ”1**

CHASE CUNNINGHAM

**首席分析師，FORRESTER Research**

識別

## 發現、分類、清查所有連網設備

有了Forescout平台，安全和IT運營團隊可在所有IP連接的設備訪問網路時即時獲得100%的可視性，從而創建準確即時的資產清單。

- 從20多種主動和被動發現和分析特徵中篩選，適用於您的業務環境，並幫助確保持續的網路可用性
- Forescout設備雲中的12M+設備指紋特徵資料庫為您提供了高準確度的設備分類功能，可以確定設備功能、OS、供應商和型號等
- 獲得所有地點、網路和設備類型的無盲區全面覆蓋 - 無論是否具有802.1X認證

合規

## 評估安全態勢和合規性

需安裝代理程式的安全工具對代理程式缺失、損壞或無法使用的被管 理設備視而不見。此外，由於IoT設備無法支援安裝代理程式，如果這些工具無法對其進行評估 - 將進一步擴大了受攻擊面。

但通過Forescout 平台，您可以在設備連接時自動對所有具備IP的設備進行安全態勢評 估和修復，並在之後持續進行。

- 從您現有的安全工具中查找並修復代理程式缺失、損壞或無法使用的被管理設備
- 檢測設備不合規性、安全態勢變化、漏洞、弱密碼、IoC、偽冒嘗試和其他高風險指標，所有這些都不需要安裝代理程式
- 評估並持續監測非受管設備，包括不能安裝代理程式的設備，以執行安全合規

> **我們從Forescout平台上得到的資訊量是不可思議的。它確實是我用來正確尋找、識別和控制系統最好工具。它對我們來說是無價的。**
>
> **JOSEPH CARDAMONE**
> **SR.信息安全分析師，**
> **HAWORTH INTERNATIONAL**

連接

## 在異質架構網路執行訪問策略

Forescout平台基於設備和用戶身份、設備衛生和實時合規狀態實施零信任安全，而不需要改變基礎架構或進行硬體、軟體升級。

- 根據用戶角色、設備類型和安全態勢，提供對企業資源的最低訪問權限
- 防止未授權、非法和冒充的設備連接
- 在有線、無線和VPN基礎架構上實施彈性的控制 - 無論是否有802.1X

1. 零信任擴展生態系統：網絡戰略計劃：安全架構和運營手冊，Forrester Research，2019年1月2日
2. Forrester WaveTM: 零信任擴展平台提供商，2019年第4季度

**Forescout 平台以及 IoT/OT 安全能力遠高於競爭對手。最大的可視性，帶來最大的運營控制和最終的安全，是 Forescout零信任方法**

**FORRESTER RESEARCH**

## 不 要 視 而 不 見
## 而 是 需 要 立 即 防 護

馬上聯繫我們， 主動保護
您的企業物聯網。

forescout.com/platform/eyeControl　vian.chen@forescout.com　zh.forescout.com

FORESCOUT
Active Defense for the Enterprise of Things™

若需更多資訊請至Forescout TW臉書粉絲專頁或來信洽詢
郵件信箱　vian.chen@forescout.com
粉絲專頁　https://www.facebook.com/FORESCOUTtw/