FORESCOUT
Automated cybersecurity across your digital terrain

# OT 的網路安全和風險管理

## 降低風險、自動化合規性並最佳化 ICS 和 OT 環境的威脅分析

資訊技術 (IT) 和營運技術 (OT) 網路持續融合，使原本獨立工業控制系統 (ICS) 網路的複雜性和漏洞持續升高。這與工業物聯網 (IIoT) 裝置的爆炸性成長同時發生，造成巨大的能見度差距，並使得合規執行更加困難。企業、組織需要一個安全工具能夠針對 OT 和 ICS 提供精準的資產管理的能力，並且能針對營運和網路風險進行有效、即時的管理。

> **至 2025 年，75% 的 OT 安全解決方案將與 IT 安全解決方案交互運作，並透過多功能平台實現。[1]**
>
> **GARTNER**

## OT 環境的主要挑戰

隨著組織升級基礎架構、採用新技術並整合 OT 和 IT 網路，必須在現代異質網路環境中維護和保護易受攻擊的 OT 和 ICS 系統。因此，安全和營運團隊面臨的挑戰正開始浮現，包括：

- 識別、分類及控制所有受控與非受控的連網 IT 裝置、IIoT 系統和 OT 資產
- 分析警報、確定威脅的優先順序並及時回應事件，將業務中斷的風險機率降至最低
- 確保所有連網裝置，包含傳統的 OT 系統，皆能符合法規要求和監管政策
- 建立精準且最新的資產清單

# Forescout eyeInspect：IIoT 和 OT 基礎架構的網路抗災韌性和風險管理

Forescout eyeInspect ( 原名 SilentDefense™) 保護 OT 和 ICS 網路免受各種威脅，提供被動和主動探索功能，以建立自動、即時的資產清單，並根據潛在的業務影響，採取針對性的修復措施。

- 實現被動、即時的網路監控和分段
- 使用進階警報聚合的演算法 ，提升威脅分析和修復措施的效益
- 提供與 ServiceNow® 的豐富整合以及 SIEM 解決方案、防火牆、IT 資產管理、沙箱及驗證伺服器的原生介面
- 提高 SOC 和分析師的效率，以利用資產風險框架自動化風險分析
- Forescout 平台能為雲端與邊緣裝置提供卓越的裝置能見度、分類和剖析功能

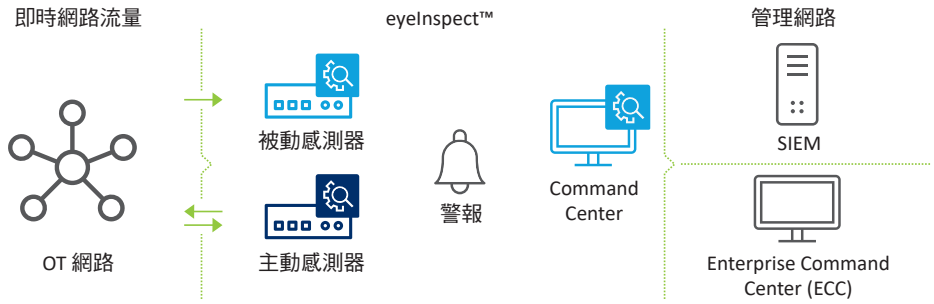


圖 1：基本 eyeInspect 部署模型

## 完整的能見度和威脅偵測

eyeInspect 將 Forescout 平台領先業界的裝置能見度、分類及剖析功能，擴展到更深入的 OT 和 ICS 環境。它可識別並有效修復各種網路和營運威脅，包括：

- 網路攻擊 (DDoS、MITM 和掃描等 )
- 未經授權的網路連接、通訊
- 可疑的使用者行為 / 原則變更
- 裝置故障或不當的組態設定
- 新的和無回應的資產
- 毀損的訊息
- 未經授權的韌體下載
- 不安全的通訊協定
- 預設的憑證和不安全的驗證
- 邏輯變更
- 具 IP 功能和序列裝置的能見度

## eyeInspect 使用案例

### 資產能見度和監控

eyeInspect 提供跨 OT 網路和站台的持續性資產能見度。它可自動建構詳細的網路地圖，包括豐富的資產詳細內容，並依照網路 / 角色自動分組，以 Purdue 層級和通訊關係等多種格式提供。eyeInspect 採用廣泛的探索功能，包括：

- 獲得專利的 150 多種 IT 和 OT 通訊協定深度封包檢查
- 持續且可設定的原則和行為監控
- 自動評估裝置漏洞、威脅暴露、網路問題及營運問題
- 可選的非侵入式主動組件，以選擇性地查詢特定主機

### 資產配置管理

eyeInspect 自動收集各種 OT 資產資訊，記錄所有配置變更以進行安全分析和操作鑑識。可探索的詳細資訊包括：

- 網路位址
- 主機名稱
- 資產的製造商和型號
- 序號
- 作業系統版本
- 韌體版本
- 硬體版本
- 裝置模組資訊

### 自動化合規

藉由 eyeInspect 主動感測器，資產擁有者可根據特定的合規原則，輕鬆對資產和資產群組建立基準，以自動偵測與既定基準的偏差。這些基準可讓您根據組織需要或合規指南 ( 例如 NERC CIP、ISA99/IEC 62443、NIS 和 NIST CSF 以及 FDA 和 FIPS) 定義自訂的基準原則。資產擁有者可以為這些合規框架產生可接受的基線證明 / 報告。

### 網路存取控制和分段

eyeInspect 運用 Forescout 平台的 ACL 和 VLAN 指派功能，將基於政策分段和存取控制引進作業網路，以支援跨 IT、物聯網和 OT 的統一且即時的資產管理。透過 eyeInspect，資產擁有者可對 IT、OT 和醫療保健環境的資產之間的關係 ( 通訊模式 ) 進行情境感知 ( 即通訊協定感知 /DPI) 映射和視覺化，並可整合其他現有的流量遙測系統 / 產品 (Medigate、NetFlow、SPAN 等 )。

### OT 網路彈性帶來的獲利效益

Forescout eyeInspect 可透過提升其作業系統的安全性和彈性，同時大幅強化管理效率、風險管理和合規性，對組織的獲利產生正面影響。

例如，Forescout 最近研究 OT 網路監控對美國某著名食品生產公司財務績效的貢獻，該公司擁有 17 名著重於 ICS 網路安全和合規性的全職員工。2 研究發現：

- 在降低勞動力成本、提高管理效率，以及改善與資產和網路能見度相關的威脅獵捕能力方面，每年可節省 820,336 美元。
- 與可據以行動的威脅管理更新、更快的事件回應，以及減少停機風險等相關的每年節省為 346,456 美元，這些都與更強大的網路威脅偵測和回應能力有關。
- 與 ICS 安全和資產管理解決方案的內建整合相關的合規成本，每年可節省 158,120 美元。

## 威脅偵測和事件回應

利用 eyeInspect 的警報調查和回應工具，自動偵測、遏止及修復威脅。儀表板和小工具可強化使用者協作。豐富的警報詳細資訊可支援根本原因分析，並加快有效、高效的回應。Enterprise Command Center (ECC) 可讓使用者仔細檢視來自任何多站點或地點分散網路的警報，以詳細分析事件，包括涉及的裝置和警報的來龍去脈。


圖 2：eyeInspect 是 Forescout 統一 IT-OT 安全平台的一部分，此平台為整個企業的網路和營運風險提供狀況感知及自動控制。

# 不要視而不見。保護它。™

**立即與我們聯絡，積極捍衛您的企業物聯網。**

1. Gartner 營運技術安全市場指南 (Gartner Market Guide for Operational Technology Security)，2021 年 1 月 13 日
2. 基於標準化客戶資料的預測。實際節省效果依據多重因素而有不同。

forescout.com/platform/eyeInspect　salesdev@forescout.com　免付費電話：1-866-377-8771

FORESCOUT
Automated cybersecurity across your digital terrain

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

免付費電話 ( 美國 )：1-866-377-8771
電話 ( 國際 )：+1-408-213-3191
客服電話：+1-708-237-6591

若需更多資訊，請至 Forescout.com