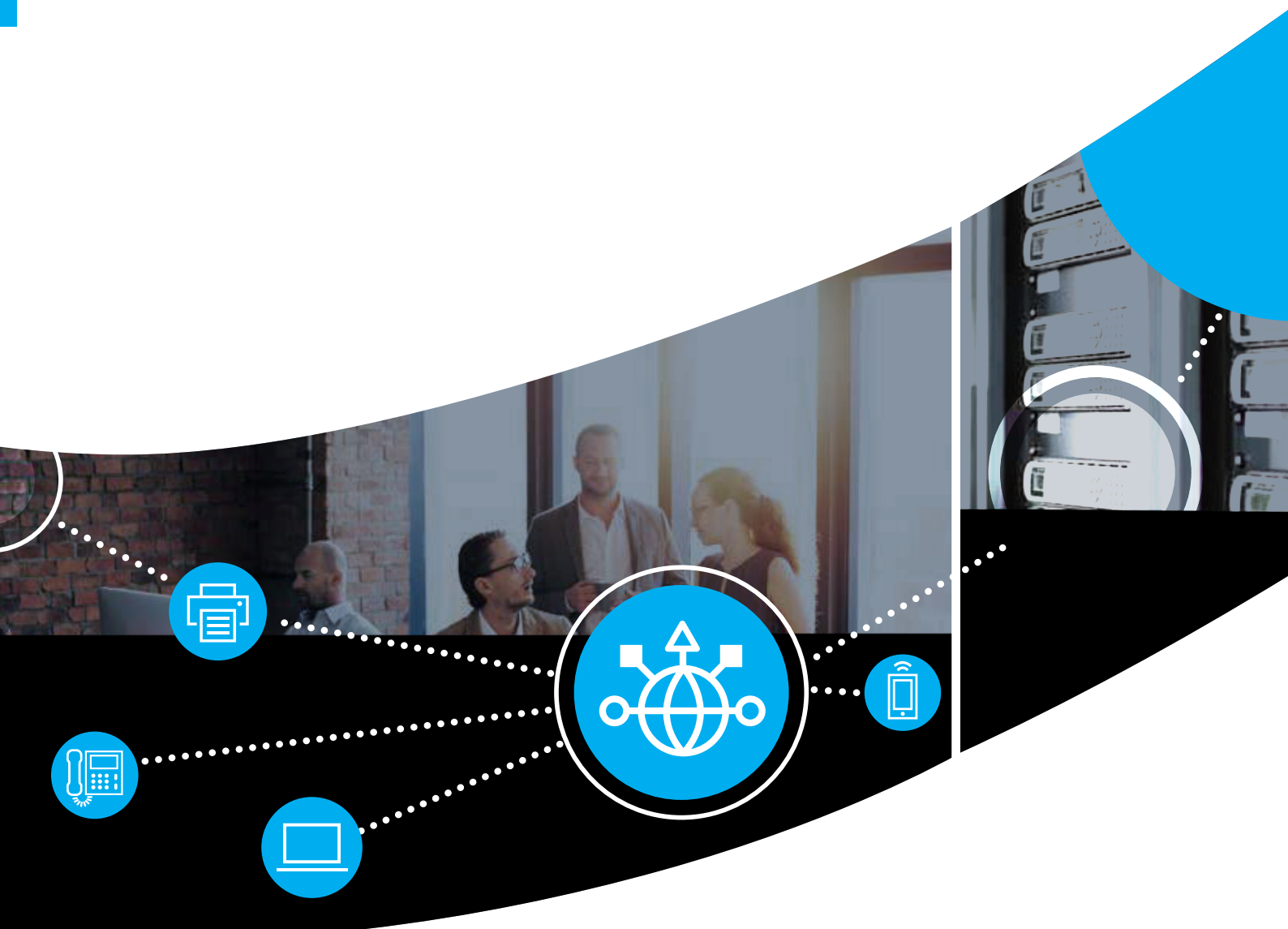
ForeScout

ForeScout

視覺化浪潮下的安全新趨勢

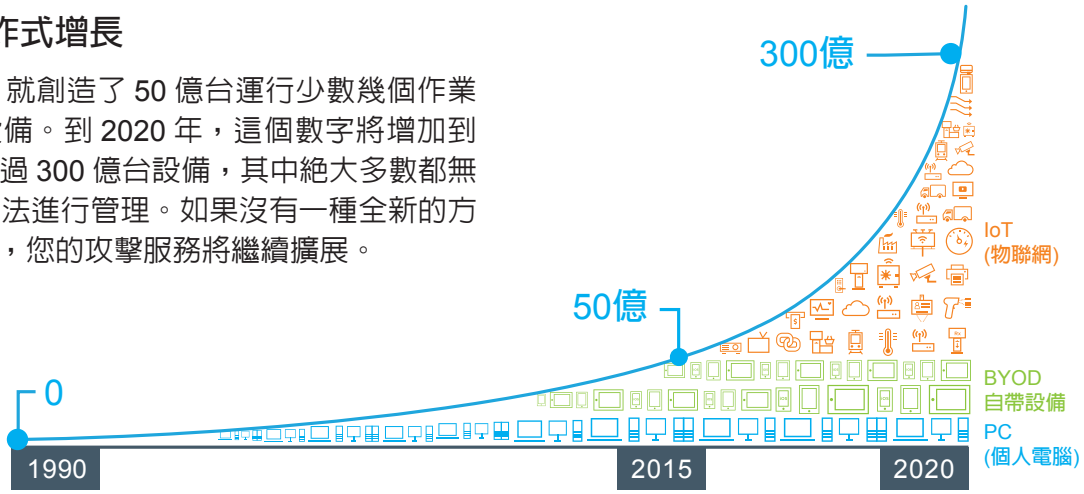


可視

挑戰：

平臺和 IoT 設備呈爆炸式增長

僅僅用了二十五年時間，就創造了 50 億台運行少數幾個作業系統（OS）的網路連接設備。到 2020 年，這個數字將增加到運行數百個作業系統的超過 300 億台設備，其中絕大多數都無法使用基於代理的安全方法進行管理。如果沒有一種全新的方法，網路盲點將成為常態，您的攻擊服務將繼續擴展。



ABI Research，2017
物聯網（IoT）、新作業系統和移動性的高速發展正在引發非受管設備的爆炸式增長。

解決方案：

無代理可見性和控制

ForeScout 開創了一種無代理的安全方法，可即時發現設備並對設備進行分類、評估和監控，讓您可以看到網路上的全部設備（從校園到雲），並對其進行安全管理。

應對措施：

當前的業務不是在標準、一成不變的網路上運營的，而是隨著時間不斷地發生動態變化。在 ForeScout，我們推出了為整個網路提供可見性的異構安全性，範圍從校園內設備到資料中心和私有 / 公共雲環境中的工作負載。我們的方法高度靈活且與供應商無關，可支援 Cisco、Aruba、Juniper Networks 和運行 802.1X、非 802.1X 或同時運行二者的其他有線和無線網路。

安全性的前提是要瞭解您的網路上有什麼。我們會發現您的基礎設施、物理 / 虛擬系統、受管 / 非受管端點、IoT 和未授權設備，而無需使用軟體代理或瞭解以前的設備。接下來，我們的解決方案將評估設備安全性，並持續監控安全狀態。

我們的適應性資料收集功能支援您選擇資料集，並使用右側列出的高級的主動和被動技術獲得深入的可見性。我們的解決方案可快速評估設備和應用程式，確定設備使用者、所有者、作業系統、配置、軟體、服務、修補程式狀態和是否存在 安全代理。瞭解這些資訊可讓您執行準確的存取控制、實施和修復策略。

ForeScout 如何說明您監測更多情況

1. 輪詢交換機、VPN 集中器、接入點和控制器，以提供連接設備的清單
2. 從交換機和控制器接收 SNMP 陷阱
3. 監控對內置或外部 RADIUS 伺服器的 802.1X 請求
4. 監控 DHCP 請求，以檢測新主機何時請求 IP 位址
5. 可以有選擇地監控網路交換機埠分析器埠以查看網路流量，例如 HTTP 流量和橫幅
6. 運行網路映射器（Nmap）掃描
7. 使用憑據在設備上運行掃描
8. 接收 NetFlow 資料
9. 導入外部媒體存取控制位址分類資料或請求 LDAP 資料
10. 監控公共 / 私有雲中的虛擬機器
11. 使用乙太網供電和 SNMP 對設備進行分類
12. 使用可選代理

解決最棘手的使用案例

物聯網 (IoT)：

在 IoT 設備連接到您的網路時立即發現該設備，而無需使用代理。對設備、使用者、應用程式和作業系統進行分類和分析，並自動分配設備以保護虛擬區域網路（VLAN）段並監控行為。

網路存取控制：

在設備、使用者、應用程式和作業系統訪問您的網路時獲得即時可見性。將問題通知給用戶和 IT 工作人員，並自動應用適當的存取控制，例如限制、阻止、隔離設備，或將設備重新分配給 VLAN 段。

訪客聯網：

自動完成訪客、承包商和合作夥伴註冊，並使用適當的登入選項實施策略合規性。與企業移動管理和端點保護工具共用設備安全狀態詳細資訊並協調實施操作。

BYOD 安全：

在員工將自己的筆記型電腦、平板電腦和智慧手機連接到您的網路時提供無代理可見性。實施存取控制和端點合規性策略，從而消除與打開或關閉網路埠相關的手動操作。

端點和法規合規性：

在設備進出網路時監控設備，並向使用者通知策略違規情況，例如過期或不合標準的安全軟體、作業系統和配置設置。自動將用戶重定向到自修復門戶。

安全的雲計算：

將校園中設備和虛擬機器的可見性和控制擴展到您的私有和公共雲環境中。在物理環境和虛擬環境中使用單一窗格視圖，從而可以利用現有安全操作的團隊技能和流程。

控制

> “到 2020 年，利用即時發現、可見性和控制機制來保護 IoT 的組織將從今天的 5% 至少上升到 25%。”
>
> — Gartner，即時發現、可見性和控制對 IoT 安全至關重要，Saniye Burcu Alaybeyi 和 Lawrence Orans，2016 年 11 月 3 日

挑戰：

安全警報太多，實施能力不足

大多數安全工具在發送警報方面非常出色，但卻沒有能力實施操作。因此，安全團隊因必須手動評估和處理大量警報而不堪重負。有些警報會生成誤報並被忽略，而其他警報則會由於資源限制而蒙混過關。

解決方案：

基於策略的分段和實施

ForeScout 可對設備、使用者和應用程式自動完成基於策略的存取控制和實施，從而允許您限制對適當資源的訪問、自動完成訪客登入、查找和修復端點安全性漏洞，並幫助維護和改進行業法規合規性。

應對措施：

ForeScout 允許您根據策略和情況的嚴重程度，將廣泛的主動操作或被動操作自動化，並對連接實施控制。為了實現這一點，我們使用策略引擎來持續地基於一群組原則檢查設備，這群組原則指示並實施網路上的設備行為。與其他供應商定期檢查或查詢設備的產品不同，我們的策略引擎可以即時監控單個部署中超過一百萬台設備的行為。

策略是基於特定設備上發生的事件而被觸發的。這些事件可以是網路准入事件（插入交換機埠或 IP 位址更改）、身份驗證事件（由 RADIUS 伺服器接收或通過網路流量檢測）、使用者 / 設備行為更改（禁用防毒軟體、添加禁用的週邊設備、打開 / 關閉埠）以及特定的流量行為（例如設備通信方式以及所使用的協定。）

通知

- 電子郵件使用者 / 管理員
- 發送螢幕通知
- 重定向到網頁
- 請求最終用戶回應
- 發送系統日誌 / CEF 消息
- 開立幫助台票證
- 與 IT 系統共用情境

確認

- 移動到訪客網路
- 更改無線用戶角色
- 分配給自修復 VLAN
- 限制未授權設備
- 啓動應用程式 / 進程
- 更新防病毒 / 安全代理
- 應用作業系統更新 / 修補程式

限制

- 隔離設備
- 關閉交換機埠
- 阻止無線或 VPN 訪問
- 使用 ACL 限制訪問
- 終止未授權的應用程式
- 禁用 NIC / 週邊設備
- 觸發修復系統

ForeScout 可以根據您的安全性原則實施適當的控制級別，從適中到嚴格。

自動化

挑戰：

分段安全

大型企業會有數十個未連接、分散的安全系統。這種孤立的方法阻止了協調一致、企業範圍的安全回應，從而使攻擊者有更多的時間來利用系統漏洞。

> “在深夜，或者當我的工作人員睡覺時，ForeScout 正在與我們的其他安全解決方案合作，發現威脅並立即採取行動。這種自動化功能的價值是無法用金錢來衡量的。”
>
> — Michael Roling，首席資訊安全官，密蘇里州

解決方案：

安全自動化

ForeScout 使用領先的 IT 和安全管理產品來協調資訊共用和基於策略的安全實施操作，以便在無人干預的情況下實現安全工作流自動化並加快威脅回應速度。

應對措施：

通過將視覺化和控制作為基本功能，ForeScout 可以打破安全壁壘，並可利用您現有的安全投資。使用 ForeScout 模組能夠持續交換設備安全性、威脅、行為和合規性資料，使您現有的安全工具和分析更智慧、更具有情境感知能力。您的安全基礎設施可以獲得關鍵的控制功能，允許您自動實施手動策略、加快回應速度並顯著改善您的安全狀態。以下是幾個示例，說明如何通過 ForeScout 將您的工具放到我們的工具上層，以實現系統範圍的安全協調：

高級威脅檢測 (ATD)：檢測到惡意軟件和感染指標（IOC）後，領先的 ATD 產品立即通知 ForeScout 平臺。然後，ForeScout 解決方案根據策略隔離被感染的設備，並執行修復操作。它還會掃描現有設備和新設備以查找 IOC，並啓動緩解。

安全資訊和事件管理 (SIEM)：當有設備連接到網路時，ForeScout 平臺檢測到並分析該設備，然後與 SIEM 共用設備詳細資訊，使其更加智慧。SIEM 根據收集的事件和日誌對設備進行評估。ForeScout 根據您的安全性原則將此洞見轉化為操作，允許、拒絕或隔離設備。

動態網路分段：通過與領先的防火牆、交換機和路由器供應商產品深度整合，我們的策略引擎可以自動應用 VLAN 或存取控制清單（ACL），將設備和使用者放到或分配給適當的網段。對訪客、承包商、特定員工和 IoT 設備進行分段有助於防止透視、橫向、內部和 DDoS 攻擊。

有關協調功能的完整列表，請訪問 forescout.com/modules。以下是一些與我們合作的合作夥伴：

amazon web services · Check Point SOFTWARE TECHNOLOGIES LTD · CYBERARK · FireEye · IBM

McAfee · MobileIron · paloalto NETWORKS · QUALYS · RAPID7

servicenow · splunk> · Symantec · tenable · vmware

“ForeScout 在網路存取控制（NAC）技術方面取得的成就顯然具有變革性。”

— Frost & Sullivan 最佳網路安全 2016

“ForeScout 為摩根大通提供了增強的可見性和控制能力，可以監控連接到我們公司網路的數十萬台設備。”

— 摩根大通公司全球首席資訊安全官 Rohan Amin

公司概況

行業：網路 / 物聯網安全

客戶：全球 60 多個國家 / 地區內的 2000 家企業和政府機構 *

市場：金融服務、政府和國防、醫療保健、製造、教育、零售和關鍵基礎設施

成立時間：2000 年

CEO：Michael DeCesare

2016 年榮獲的獎項和讚譽：

- 摩根大通變革性安全技術名人堂創新獎。
- Gartner IoT 安全市場先鋒。
- Gartner NAC 市場先鋒。
- 福布斯 100 強雲技術公司。
- Deloitte 科技發展最快 500 強。
- Nanalyze 9 大熱門網路安全創業公司之一。
- CRN（電腦經銷商新聞）雜誌最強安全公司。
- Inc. 成長最快 5000 公司之一。
- SC Magazine 歐洲最佳 NAC 解決方案。

安全框架 / 合規性要求：

領先的安全標準體系和框架有一個共同的基本原則：安全性從可見性開始。ForeScout 可以幫助企業和政府機構遵守以下要求：

- 互聯網安全 CSC（關鍵安全控制）中心。
- CDM（持續診斷與緩解）。
- FISMA（聯邦資訊安全管理法案）。
- HIPAA（健康保險攜帶和責任法案）。
- HITECH（健康資訊技術促進經濟和臨床健康法案）。
- ISO/IEC 27001（國際標準組織和國際電子電機委員會）。
- NIST（國家標準與技術研究所）風險管理框架。
- PCI-DSS（支付卡行業資料安全標準）。
- SCAP（安全內容自動化協定）。
- SOX（薩班斯 - 奧克斯利法案）。

Westcon Solutions

新加坡商威實康科技-台灣分公司
台北市內湖區洲子街112號4樓
TEL：(02)8751-8026
FAX：(02)8751-8022
Email：wstw@westcon.com
www.tw.westcon.com
www.westconsolutions.com

ForeScout

* 截至 2016 年 12 月 31 日