FORESCOUT
Automated cybersecurity across your digital terrain

Forescout
落實政府推動零信任策略

符合NIST SP 800-207準則的零信任基礎

零信任

越來越多的企業安全策略以及安全解決方案業者的開發藍圖，有充分的理由採用資訊安全零信任模型，在無邊界網路的趨勢下，企業有更多的行動與遠端工作者與大量的物聯網裝置，以往預設信任內部網路的架構並不適合新的需求。

邊界安全越來越式微

現在的企業環境嚴重高度仰賴雲端服務、生態系統中的合作夥伴和行動員工，全都位於原有網路邊界外。且使用者、物聯網裝置及應用程式存取更多的訊息，包含帳戶、資料和資源，數位轉型需要更高的靈活性。根據 Gartner 指出：「由於致力於數位轉型，大多數企業在企業外部擁有的應用程式、服務和資料將多於內部。」[2]

可視性是保護任何有價值資產的關鍵。您無法保護看不到的事物。您對整個商業生態系統的網路可視性愈高，就愈有可能快速偵測到進行中的違規跡象並予以阻止。[1]

FORRESTER RESEARCH

vian.chen@forescout.com

同時，連接網路裝置數量和多樣性，傳統端點管理方法無法勝任。許多這些連接的裝置， 包括 BYOD 和訪客、物聯網裝置及 (OT) 運作系統，無法安裝或執行裝置管理程式，礙於安全團隊無法看見這些裝置，因此無法識別這些設備或其使用者、評估其安全狀態或控制。

邊界安全為主的系統缺點，讓 Forrester Research 分析師發展零信任作為替代方案。零信任概念和架構模型於 2010 年發表，讓安全團隊了解應如何重新設計具備安全的微分段網路，使用混淆技術加強資料安全、給予使用者適當的訪問和存取權限降低相關的風險，並透過分析和自動化大幅提升安全偵測和回應能力。

零信任：從概念模型到完整的框架

零信任模型最早僅關注於分段保護及最小存取控制權限的概念，對於如何在實際環境中利用現有安全控制方面，幾乎沒有任何具體的方向。隨著時間發展，基本模型已進化成熟，成為 Forrester 稱之為 ZTX (Zero Trust eXtended) 的零信任擴展生態系統，此完整框架確立了 ZTX 的七個關鍵元件：網路、資料、人員、應用程式前後端、裝置、可視性和分析，以及自動化和應變。

零信任擴展生態系統的元件

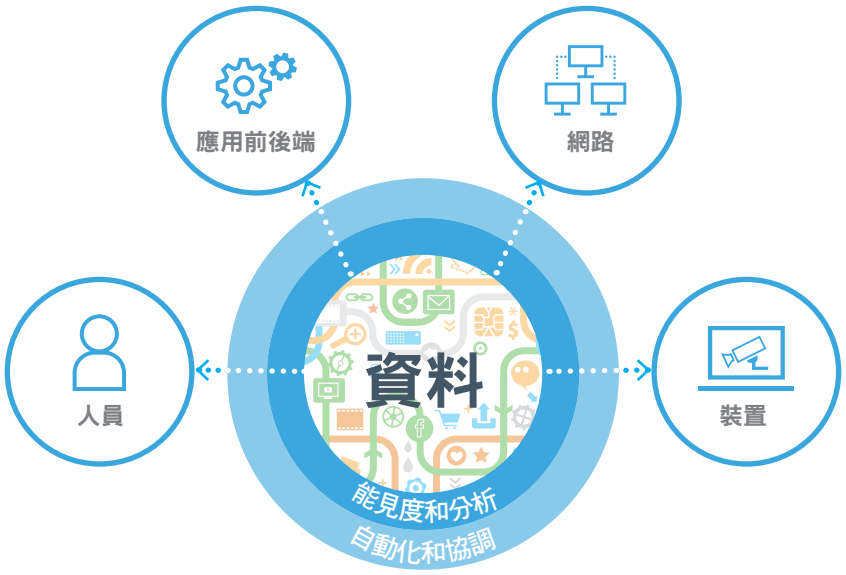

圖 1：Forrester 的零信任擴展生態系統包括七個必要的層面。

ZTX 框架協助安全團隊瞭解以技術達成下列目標：

- 實現網路隔離、分段和安全原則
- 實現資料分類、隔離、加密和控制
- 保護網路和基礎架構資源的使用者 (人員和物聯網)，同時從使用者端保護這些資源
- 保護公有雲和私有雲中的前後端應用
- 異質環境零信任控制和程序的自動化及協調
- 提供可視性和分析，清楚呈現並將保護延伸到企業所有角落

可視性對於成功的零信任架構極為重要

零信任策略的基本原則是探索並分類所有連網裝置，不只是已安裝並執行端點代理程式的裝置，並根據精細的裝置分析、使用者身分和授權、軟體堆疊、組態合規性和安全態勢，嚴格執行最低權限存取原則。為了執行存取控制原則，首先必須檢視並評估網路上的所有事物。

Forrester 強調零信任中的可視性主題。Forrester 分析師 Chase Cunningham 表示：「可視性是保護任何有價值資產的關鍵。您無法保護看不到的事物。您對整個商業生態系統的網路可視性愈高，就愈有可能快速偵測到進行中的違規跡象並予以阻止。零信任要求對整體業務的可視性和分析進行大量投資。」[1]

若要實現這樣的策略，需要完整的裝置可視性和控制解決方案，能夠檢視並控制所有聯網事物，包括傳統端點管理系統無法檢視和控制的裝置：BYOD 和訪客裝置、停用代理程式的企業端點、惡意裝置、物聯網裝置、網路交換器和路由器、廠區和其他 OT 系統，以及公有雲中的虛擬機器。

Forescout 解決方案：完整的裝置可視性和控制

Forescout 的解決方案將領先的網路技術進化成零信任平台。事實上，在其最新的零信任安全手冊中[1]，**已將 Forescout 稱為零信任平台，這歸功於與 Forrester 的基礎功能與 ZTX 框架幾近吻合**。

Forescout 平台是一種無代理程式的安全解決方案，可在網路端點連接至網路時，對其進行動態識別及評估。它可以快速確認使用者、所有者和作業系統，以及裝置組態、軟體、服務、修補程式狀態及安全程式的存在（或缺少）。其次，它提供對這些裝置的矯正、控制及持續監控。

Forescout 解決方案可用於納管的企業裝置、未被納管的訪客裝置、實體及虛擬伺服器、網路基礎設備、工業營運和控制系統 (ICS）以及物聯網裝置（IoT），無須代理程式或事先針對裝置設定。可以快速部署至您現有的環境中，幾乎不需要更改基礎架構、升級或重新設定端點。更重要的是，它可以在實體、虛擬及混合雲環境中無縫運行。無縫運作。

零信任平台標準

FORRESTER 將零信任平台定義為：
• 在至少四個零信任元件中提供領先市場的功能
• 為解決方案整合創造獨特的技術優勢
• 開發並支援強大的 API 和合作夥伴生態系統
• 維持可視性、分析、原則和自動化的重心

「物聯網和支援網路的裝置技術已為網路和企業帶來潛在危害……安全團隊必須持續隔離、保護和控制網路上的每個裝置。」[3]

FORRESTER RESEARCH

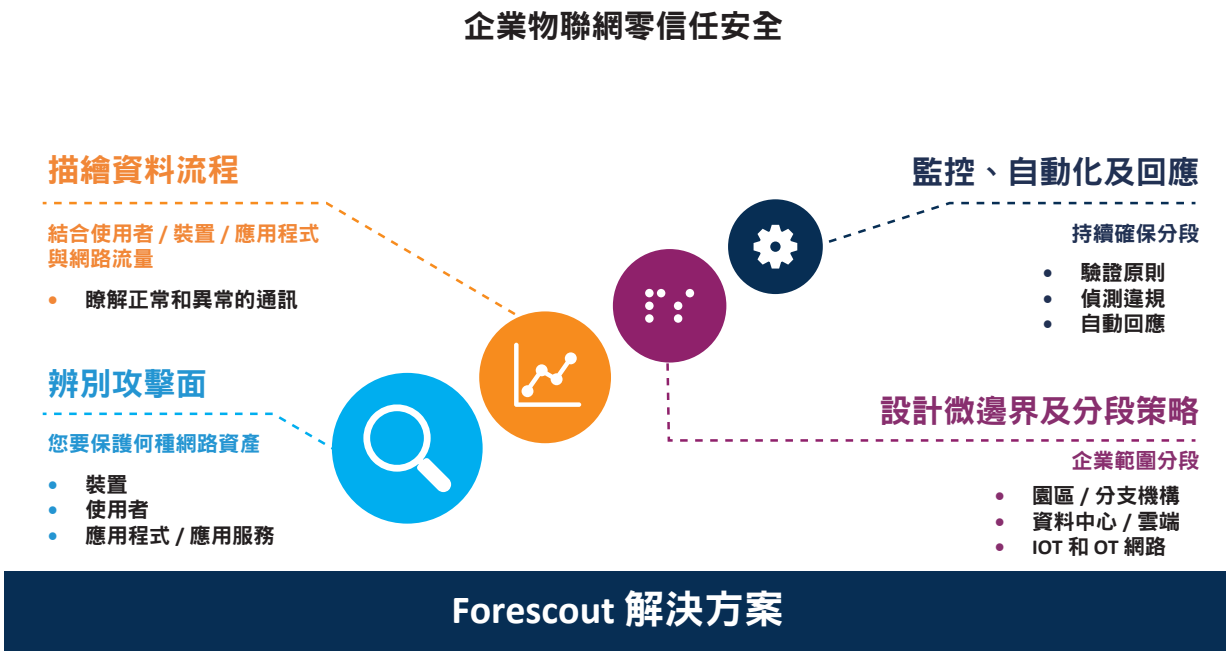

圖 2：Forescout 平台使用無代理程式可視性、存取控制、動態網路分段和安全聯防，在您的企業物聯網中實施零信任安全，無論使用者或裝置位於何處。

零信任裝置可視性、分段及控制

Forescout 平台能完整發現所有 IP 連網裝置及分類，並持續做風險與安全評估，以確定每個連網裝置的即時狀態。然後運用這些資訊以自動規則控制，並與設備進行連動。這些功能為有效的零信任安全提供了基礎。

透過無代理方式發現所有設備。Forescout 平台採用無代理程式方式，整合主動和被動方式，發現病分類組織內網路 - 從園區、資料中心、雲端以及 OT 網路上的所有裝置。可以偵測到個人電腦和筆記型電腦、實體和虛擬伺服器、行動和物聯網裝置、雲端執行個體及營運技術系統，無須特定廠商的網路設備，而且無論是否有 802.1X 驗證，皆無須升級現有架構或重新設定交換器和連接埠。

從裝置發現到資產資訊。Forescout 的各種探索和剖析方法可快速產生並持續更新有關裝置身分、狀態和行為的大量資訊。這些資訊提供環境中所有資產的詳細資料，為廣泛的決策和行動提供協助和訊息，並為降低風險的控制提供基礎。此外，Forescout 平台可監控並將裝置和資料來源之間的通訊、系統互依性以視覺化呈現，這對於分段對映、規劃和原則建立至關重要。

持續可視性和基於政策的裝置控制。Forescout 平台的政策引擎使用此資產資訊，以持續評估裝置是否合規，規則可根據裝置的網路許可、驗證及其他可自訂項目即時觸發。例如， Forescout 平台可識別具有對外 Internet 存取權限的新物聯網裝置，並自動將其分配到受限的網路區段。它可偵測裝置安全狀態的變化，例如已停用或異常的防毒代理程式或加密軟體。此平台會在裝置連網後以及每次連上網路時重新評估裝置。它與第三方系統共享裝置即時資訊並啟動狀態評估，例如重新掃描裝置以找出漏洞和入侵指標。

Forescout eyeControl 可直接在裝置上或透過網路基礎架構執行控制 (如下所述)。基於主機的控制包括啟動和停止應用程式、更新防毒、安全程式、停用周邊裝置，以及要求使用者確認。必要時，Forescout 平台可透過與第三方工具的連動，自動執行矯正措施，例如裝置修補或重新對裝置做漏洞評估、端點保護、加密或其他安全軟體 (同樣將在下面更詳細介紹)。

圖 3：Forescout 的分類程序會擷取所有 IP 連網裝置的詳細資料。

零信任裝置

組織面臨的最大挑戰之一是發現並保護出現在其網路上的大量的未管理的裝置。物聯網裝置的爆炸性增加，使 IT 和安全人員忙於解決 Forrester 所描述的「潛在大規模入侵目標」。[3] 隨著 IT-OT 環境融合的增加，不同的技術和責任領域之間不再有嚴格的劃分。此外，除了無法管理外，OT 設備不再因安全目的使用實體隔離。資訊長首當其衝受到這些結構性變化的影響，他們需要先進的技術在目前充滿弱點的融合環境中佔據上風，Forescout 用於裝置可視性及控制的無代理及被動探索技術能勝任需要。這些功能使該公司領先物聯網安全市場，非常適合無干擾的發現及管理 IT 和 OT 裝置。

透過將 Forescout eyeInspect 加入產品組合，Forescout 將其基於網路的狀況感知擴展到 IT 環境之外，深入到 OT 和工業控制系統 (ICS) 中。內建 100 多種 IT/OT 通訊協定的深度封包擷取 / 檢查、網路映射、流量分析、原則和行為監控、網路鑑識、威脅評估及風險評分功能。

在物聯網和 OT 安全性方面的專業知識已獲得 Forrester 的認可。事實上，根據分析機構的說法：「Forescout 是專注於零信任物聯網 IOT/OT 安全性的廠商。IOT/OT 裝置安全性是企業內部最難解決的問題之一，Forescout 是最佳選擇，其 IOT/OT 安全平台和功能在競爭對手中脫穎而出。最大的可視性可帶來最大的營運控制以及最終的安全性，Forescout 實現零信任方法的關鍵。」[4]

「Forescout 是專注於零信任物聯網 IOT/OT 安全性的廠商。IOT/OT 裝置安全性是企業內部最難解決的問題之一，Forescout 是最佳選擇，其 IOT/OT 安全平台和功能在競爭對手中脫穎而出。」[4]

FORRESTER RESEARCH

零信任網路功能

動態網路分段。微分段是零信任框架的核心原則。然而，在橫跨分散式的網路內設計、實行及維護有效的分段原則，是一個艱鉅的過程。

傳統的分段解決方案是勞動密集型，需要手動分析流量和紀錄以瞭解流量相依性。此手動方法會增加人為錯誤、不一致的分段原則，甚至造成業務中斷的可能，特別是大多數分段橫跨多廠牌設備 / 多網域的複雜企業網路環境中，會成為一項艱鉅的任務。

Forescout 的分段策略支援以應用程式、裝置 / 角色或邊界為中心的方法，實現跨企業網路環境 (園區、資料中心、IT/OT 及雲端) 所有網域的以策略為主的零信任分段。

為了簡化並加速分段的實行，Forescout 已建立一個依條件帶動的多層架構，涵蓋目前由應用程式、使用者、裝置和服務組成的多樣化使用情境。此三層架構使 Forescout 平台能夠主動識別、分段及強制執行每個連網裝置的合規性。

圖 4：Forescout 建議以三層架構作為全企業網路分段的最佳實務，從由 Forescout eyeSegment 提供支援的「原則層」開始。

透過結合 Forescout 平台和網路分段的多層方法，客戶可獲得企業網路環境全方位完整狀況，並可透過分段連動以全面降低網路和營運風險。

- **原則層：**Forescout eyeSight 不需透過代理程式，可以發現及剖析受管、非受管、 IoT / OT 裝置、虛擬執行個體和雲端應用，可讓企業對所有 IP 連網系統建立零信任基礎。Forescout eyeSegment eyeSight 為基礎，可將使用者、應用程式、服務和裝置之間的流量和相依性以使覺化方式呈現，然後透過設計、模擬及控管規則，瞭解對現有環境的影響，進而加速企業中動態網路分段的設計、規劃和部署。
- **控制連動層：**第二層協助透過不使用設備廠商專屬技術的方式，連動跨底層強制執行技術和網路網域的規則。作為領先的網路存取控制解決方案，Forescout eyeControl 提供基於規則的分段指派，與園區、資料中心和雲端環境中的首要的交換器、路由器和政策執行點協同運作。Forescout eyeExtend 產品有助於簡化控制連動層內的整合。
- **強制執行層：**第三層連動多種供應商強制執行點，以執行跨實體和虛擬網路的分段控制。此架構層還可讓客戶繼續利用並保障現有設備投資。

真實環境中，建置零信任的最重要的關鍵區別是無代理程式 (agentless)，Forescout 平台可以發現、評估和規範任何傳統 IP 連網裝置的網路存取，隨著越來越多的 Windows 作業系統終止支援服務，這一點變得至關重要。

零信任存取代理者

Forescout 平台透過網路基礎架構強制執行裝置控制操作，基於其對使用者身分、角色、驗證和裝置狀態的整合資訊，為網路存取設定和指派分段提供集中的代理服務和決策點。原生整合來自 30 多家交換器和無線廠商的產品，並提供直接整合執行於 Linux 作業系統的路由器。此技術在網路交換器上運作，可變更 VLAN、新增 ACL 或停用交換器連接埠。在無線控制器上，它可將 MAC 位址列入封鎖清單或變更使用者的角色。此外，我們的技術可限制遠端 VPN 使用者。

真實環境中，建置零信任的最重要的關鍵區別是無代理程式 (agentless)，Forescout 平台可以發現、評估和規範任何傳統 IP 連網裝置的網路存取。Forescout 產品檢視及控制每個 IP 連網裝置，並整合所有 IT 和 OT 網路基礎架構。

零信任自動化和連動功能

Forescout 平台連動整體基礎架構的安全管理，使原本未整合的安全產品統一運作。其獨特的網路、安全性和管理交互運作技術組合，透過 Forescout eyeExtend API 整合進行擴展和放大，整合超過 70 個第三方安全和 IT 管理產品，* 組合後系統可加快反應速度、達成主要營運效率，並提供卓越的安全。

Forescout 以三種方式實現安全自動化及連動：

- **分享即時情境資訊。**Forescout 平台持續監控並與您擁有的其他安全和管理系統動態分享端點裝置身分、組態和安全詳細資料。此雙向資料交換增加檢查屬性於規則引擎，並可套用至其他工具，以強化規則和動作。
- **自動化工作流程。**Forescout 的規則引擎可讓分享過去需要跨系統並手動分析所制訂基於規則的決策。自動化這些工作流程及程序將帶來協同、即時的回應。
- **自動化回應操作。**許多安全產品 (例如先進威脅偵測系統 APT、安全資訊和事件管理軟體 SIEM，以及漏洞評估工具 VA) 可通知 IT 員工有關安全問題的資訊。Forescout 平台的與眾不同之處在於它能立即套用這些發現，觸發自動回應並強制執行其各種基於策略的控制，例如隔離裝置及修復端點以消除威脅。

零信任前後端系統

Forescout 平台藉由運用不同的基礎架構和應用程式前後端系統本身，無須代理程式即可發現、分類及剖析跨混合資料中心 / 雲端環境中的實體和虛擬伺服器。除了視覺化呈現東西向及南北向流量之外，Forescout 解決方案也能追蹤和監控混合資料中心 / 雲端環境中啟動和關閉的系統，以避免可視性資料有空窗期。它會收集虛擬機器管理程式底層資訊或雲端屬性，一路到安裝 / 執行前後端應用程式，並可使用此資訊確保僅允許獲得授權的使用者和裝置存取特定應用，以支援零信任原則。

零信任使用者功能

Forescout 平台整合目錄和身份系統，獲取可用的用戶資訊，包括角色和資源的存取授權。它將這些訊息與發現的設備設定、安全狀態和合規性進行關聯，可基於設備和用戶授予相關資源訪問的權限。該平台提供的資訊可以協助建立目錄服務及業務分類的信任區。訪問及分段控管可以確保只有經過授權的內網或遠端用戶及設備訪問適合其角色或功能的資源。使用者個人行為受到持續監控，並可整合特權管理系統，發現具有不合權限的帳號。

零信任資料功能

Forescout 藉由提供因資安政策要求所需的加密、混淆或其他安全應用程式的安裝及執行狀態的可見性，支援所有 IP 連網裝置的資料安全。如果此類應用程式未安裝或執行，可執行動作如提醒使用者、通知管理員或隔離裝置直到它修復為止。此解決方案可瞭解使用者、裝置、服務和應用程式之間即時關聯，還協助您瞭解企業中的儲存和流動資訊。

從完整設備可視性開始，成功實現零信任

Forescout 產品在不影響原有環境下，加速零信任安全實現，此安全建立在其可視性優先的基礎上。若要深入瞭解，請查看以下資源：

- **全企業分段解決方案簡介：**瞭解如何簡化零信任分段並最佳化跨異質網路的風險管理。
- **OT 網路零信任分段解決方案簡介：**瞭解如何透過先進風險管理和動態分段安全地保護擴展的 OT 網路。
- **進行測試：**透過實際測試以體驗使用 Forescout 平台前後的差異，讓您瞭解強大的使用案例並突顯 Forescout 8.2 和 Forescout eyeSegment 的新功能。
- **聯絡 Forescout 諮詢服務：**您是否正在將您依據零信任模型建構你的環境？ Forescout 顧問在產品實作、流程開發、系統整合以及網路存取和端點合規最佳實務方面，均經過完整訓練、經驗豐富並獲得 認證。

* 截至 2020 年 12 月 31 日

1. The Zero Trust eXtended Ecosystem Road Map:The Zero Trust Security Playbook (Forrester Research)，2019 年 7 月 11 日
2. Gartner Market Guide for Zero Trust Network Access，2019 年 4 月
3. Mitigating Ransomware with Zero Trust (Forrester Research, Inc.)，2020 年 6 月 8 日
4. The Forrester Wave:Zero Trust eXtended Ecosystem Platform Providers Forrester Research，2019 年第 4 季

別視而不見。保護它。™

立即與我們聯絡，積極捍衛您的企業物聯網。

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