



零信任準則X全面識別設備風險

照亮隱匿於暗處的威脅!

啟動廣域式AI智能平台自動防護戰略

- Romina Chang張恩綾
- Forescout 台灣區總經理
- romina.chang@forescout.com



近期醫療院所CrazyHunter 勒索軟體攻擊事件的攻擊流程

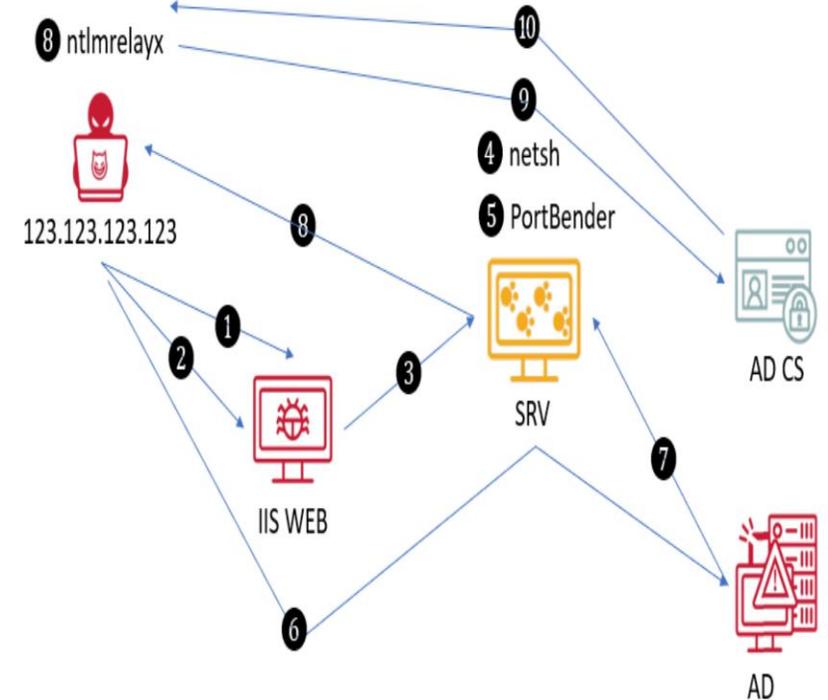
* 資料來源<https://teamt5.org/tw/posts/the-case-study-hospital-crazyhunter-ransomware-attack/>

CrazyHunter 勒索軟體的攻擊手段分析顯示其具有高度複雜性和策略性，主要包括以下技術層面的攻擊手段：

駭客入侵IIS WEB →駭客利用 IIS WEB 掃描整個網域，尋找可存取 AD 的主機→透過 IIS WEB 連線到「可存取 AD 的 SRV 主機」的 RDP(3389) →控制了一台跟IIS WEB有連線的脆弱主機(SRV)運用的 **8445端口**將流量轉發到123.223.123.123主機的**445端口**(駭客設備)

→再使用 **PortBender** 將駭客電腦 445端口流量導到有跟IIS WEB連線的脆弱主機(SRV)的 **8445端口**→駭客透過 IIS WEB 將封包傳到 AD→此時，AD 會主動反連到 SRV 的 445(SMB)，裡面有 NTLM 認證資訊→此時，445 封包會導到 8445 Port，傳至 123.123.123.123 主機(駭客設備)→駭客成功使用取得的NTLM 認證資訊NTLM 認證資訊去獲得AD machine account 的憑證→最後成功將 **AD 所有的帳號及 NTLM 取出來**→利用**AD進行端點防護卸載以及派送勒索軟體**

上述的攻擊手段是各類勒索軟體常見的攻擊流程→利用暴露網路的**各式風險設備(IT-IoT)**進入企業內網→進行橫向移動對內網脆弱設備**進行提權以及控制**→取得內網資料**利用不安全的傳輸端口**傳資料回駭客主機→**掌控AD執行勒索軟體派送進行加密以及破壞**



Forescout 平台為何能協助客戶在網路安全層次達到前期預防

- ▶ 全面識別各類設備並依據設備業務性質分類套用管制政策,確保都符合最新的安全指南，**禁用不需要的服務(通訊端口)** 如CrazyHunter案例的**445端口/8445端口**，**監控RDP&高權限帳號的連線與使用**
- ▶ **持續性的監控與自動化的矯正確保IT端點設備無重大有風險的軟體版本以及該執行的更新都有落實**，以確保端點設備有達到最佳的保護(如防毒與patch更新,無重大風險軟體)
- ▶ **Threat Detection**→設備異常行為監控
- ▶ 採用**網路分割的力量**，限制潛在攻擊的影響範圍→阻斷駭客進行橫向移動的能力

壞人使用的攻擊技巧都是相似的



所有勒索攻擊的手段都大同小異，但技術會越來越精緻與複雜

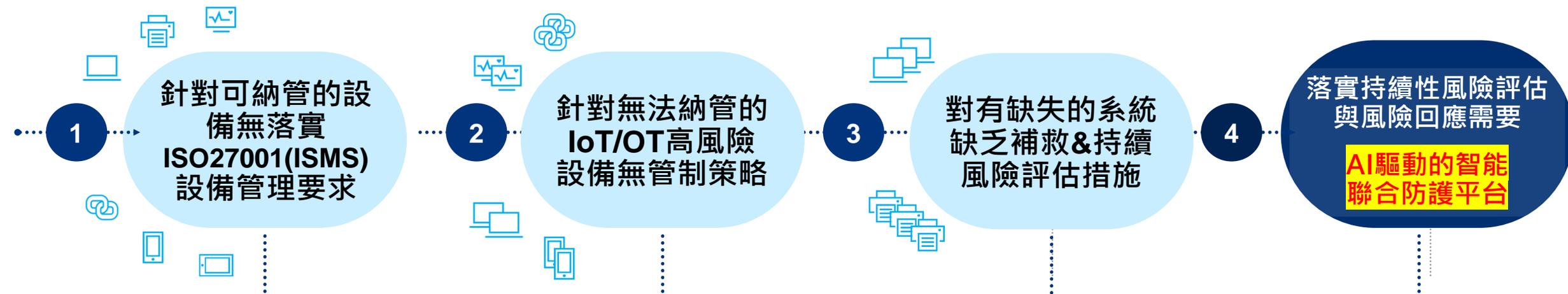


▶ 不論攻擊技巧如何演變, 勒索攻擊的手段與劇本都走相似的情境:

- ✓ 利用暴露於網路的各式風險設備(IT-IoT)當**入侵起點**進入企業內網→進行**橫向移動**對內網脆弱設備進行提權以及控制→取得內網資料後利用不安全的傳輸端口傳資料回駭客主機
→進一步掌控AD執行勒索軟體派送進行加密以及破壞,在整個攻擊行動中, 擴大勒索破壞層面

針對易受攻擊的高風險脆弱設備,無適時採取適當的風險減緩措施,導致入侵機會擴大

為何近期那些受害的企業已有傳統NAC工具、端點防護、新世代防火牆等資安工具確還沒能成功阻斷勒索攻擊?



未持續監控可納管的資產 ISMS合規性的全面落實

- a. 防毒與OS更新修補管理
- b. 高權限帳戶的變動
- c. 高風險端口的管制
- d. RDP遠端連線管制

針對無法納管的設備(如網通設備、OT、IoMT、印表機、BYOD設備)的端口管制及網路存取限制

若企業對BYOD、IoT和不易被納管設備進行分類與分割並適當地設定網路存取控制，那就面臨高風險

持續性識別與監控違反安全基準線的高風險並進行強制修補或執行嚴格的網路存取管制

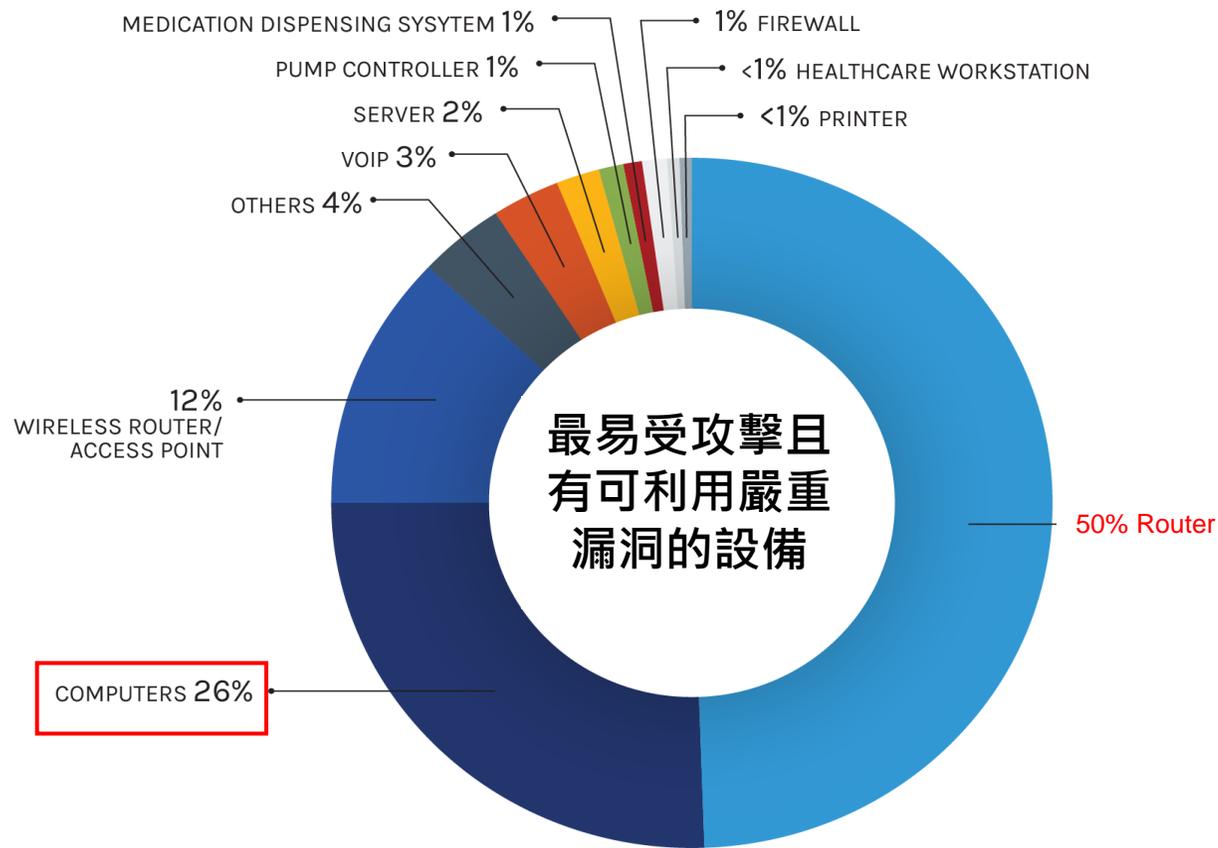
受害的單位在出事前都認為他們的管理與防護是有一定的安全性,但實際上...**存在評估的盲點**

讓有限的人力一路不斷追趕漏洞，風險無法有效解決問題!

2025 年最具風險的IP連網設備- Forescout資安研究室最新報告

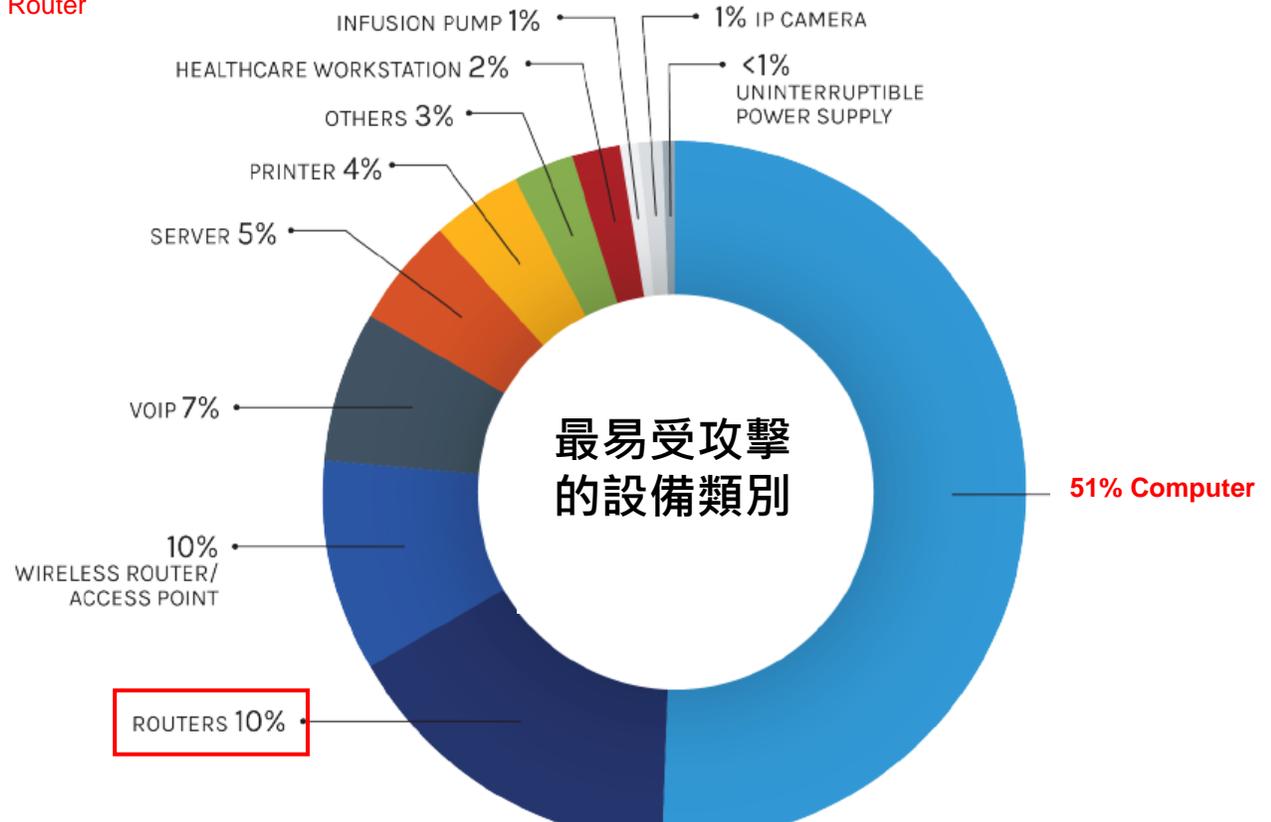
IT	IoT	OT	IoMT
Application Delivery Controller (ADC)	Network Video Recorder	Universal Gateway	Imaging Devices
Intelligent Platform Management Interface (IPMI)			Equipment
Firewall			Workstations
Domain Controller			Imp Controller
Router	Point of Sale (PoS) Systems	Uninterruptible Power Supply (UPS)	Picture Archiving and Communication System (PACS)

- 2025年的報告中有12種全新的設備類型（藍色）首次進入「最具風險設備」 -> 攻擊者對新興設備類型的興趣日益增強
- 最具風險的 IT 設備自去年起發生了顯著變化，新增了四種類型的設備：如藍色部分
- 過去端點被認為比網路基礎設施更具風險，這一趨勢在去年發生了逆轉ADC、防火牆和路由器許多高嚴重性漏洞被積極用來進行零日攻擊
- 這些高風險IoT裝置因其功能性與便利性被廣泛使用，卻常被忽略未受資安監管，因此成為駭客的主要目標



最易受攻擊且有嚴重可利用漏洞的設備
 整體而言，電腦設備的漏洞總數最多，但不是最危險的。路由器超過了電腦設備，佔最關鍵漏洞的一半。

IoMT 醫療務聯網設備（泵控制器、藥物分配系統和工作站）具有一些最危險的漏洞，凸顯了醫療業的安全風險



整體而言最易受攻擊的設備類別
 排名前十的設備類型中有五種也位列風險最高的設備之列。漏洞是連網設備的主要風險因素。整體漏洞和高度可利用漏洞之間的差異強調了為什麼**網路基礎設施和醫療設備是主要攻擊目標**。

Source: Forescout Research Vedere Labs

Forescout 4D Platform™

Forescout 4D Platform™ 持續識別、保護並確保所有管理和未管理的網路資產（包括 IT、IoT、IoMT 和 OT）的合規性，而不會干擾業務運作。它提供全面的網路安全、風險和曝露管理，以及開箱即用的第三方工具整合能力達到聯合防禦及自動化檢測和回應能力。透過生態系統合作夥伴的無縫上下文共享和工作流程協調，使您能夠更有效地管理網路風險並減輕威脅。

- ✓ 簡化風險管理
- ✓ 有效控制事件
- ✓ 快速減輕威脅



Forescout快速將你的傳統網路轉化為零信任架構



ZERO TRUST



Figure 4 - Use Case E3B2 - Forescout Discovers a Non-Compliant Network and Directs the Palo Alto Networks Firewall to Block

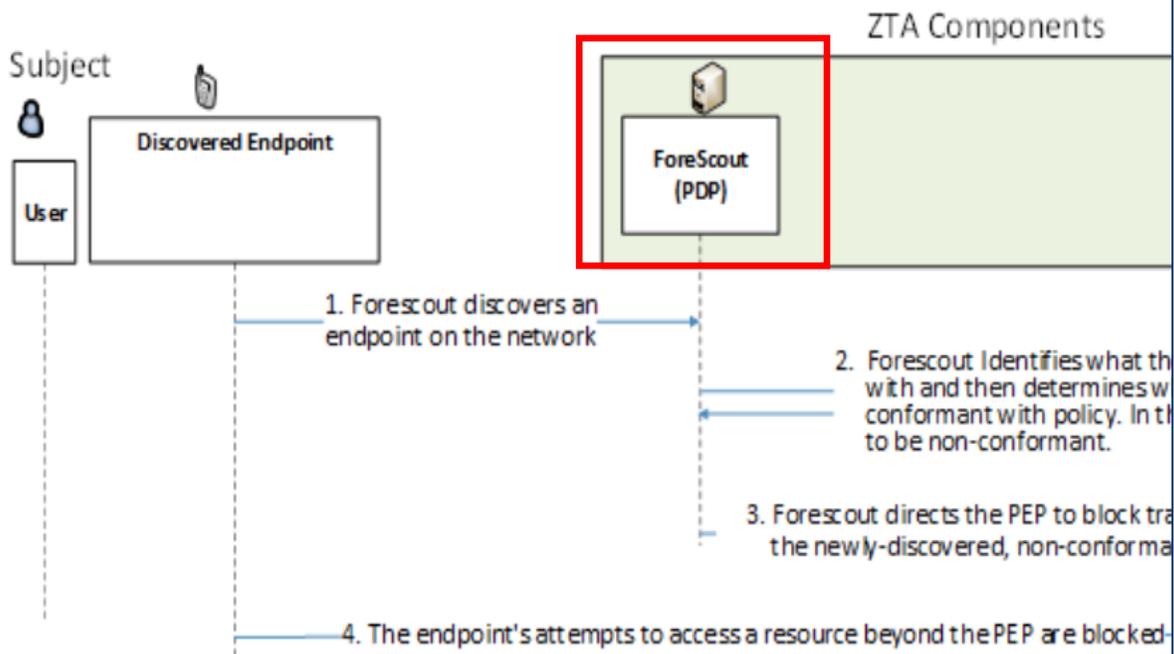
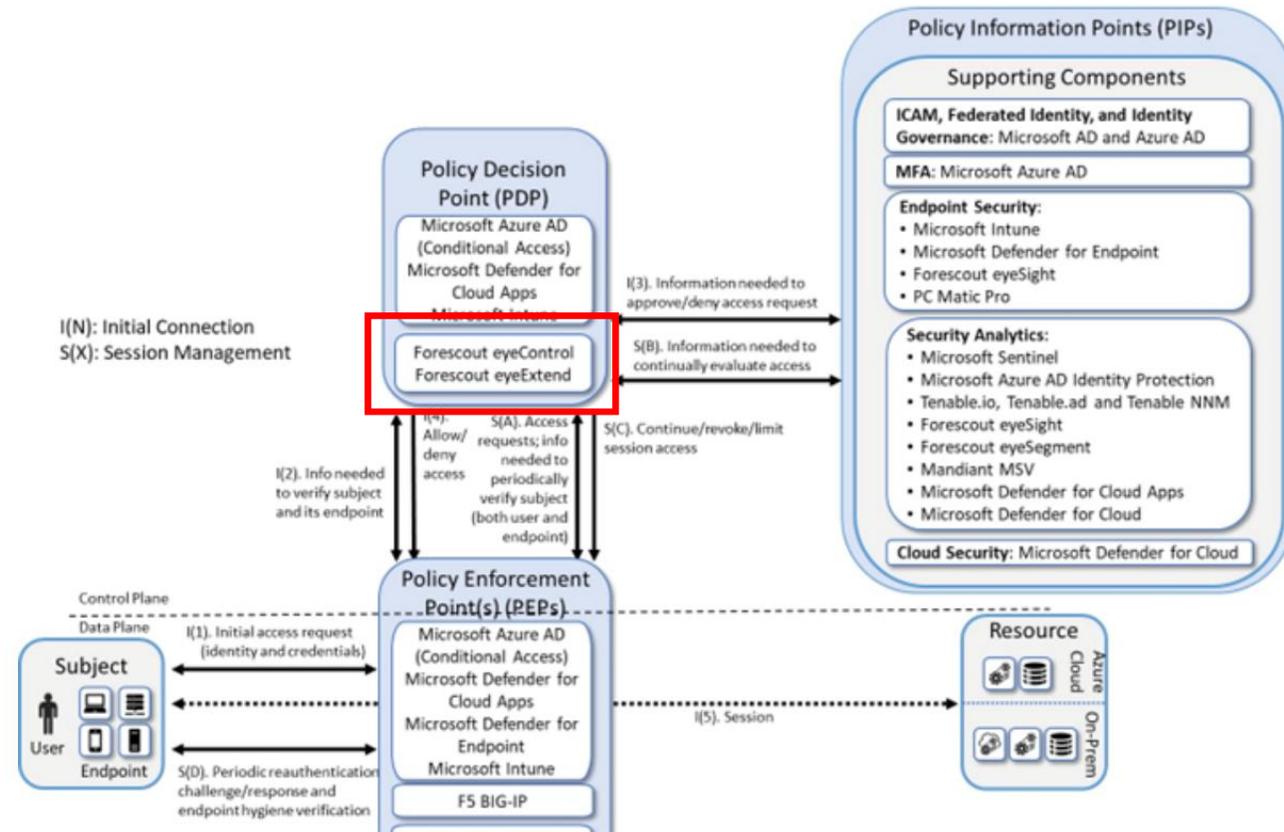


Figure 1 - Logical Architecture of E3B2

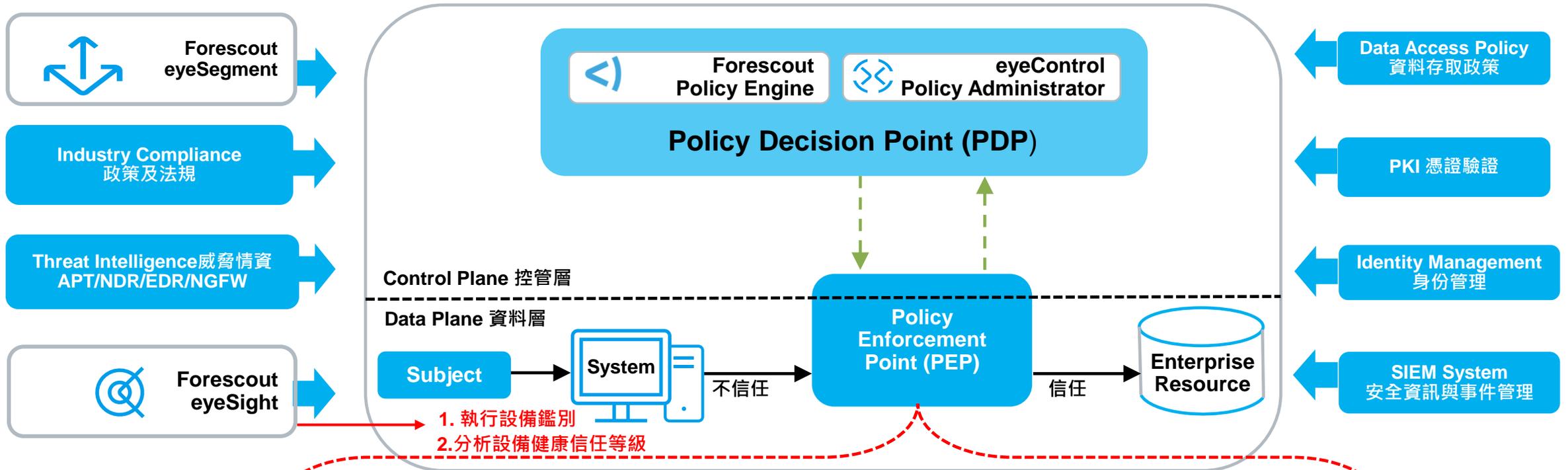


Zero Trust: NIST 800-207 零原則對應Forescout

NIST 800-207	Forescout
所有資料來源和計算服務都被視為資源	所有 IP 及其相關的使用者、應用程式、服務、裝置和機器均在 Forescout 政策引擎的範疇內
資源的存取是由動態政策決定，包括客戶端身份、應用程式/服務以及請求資產的可觀察狀態，並且可能包含其他行為和環境屬性。	此零信任原則精確描述了 Forescout Policy Engine 的運作方式。它是一種動態策略，包含盡可能多的可觀察數據來進行決策，包括來自主體、資源以及任何第三方系統的數據
企業監控並衡量所有擁有及相關資產的完整性和安全態勢	Forescout 是一個具備零信任引擎的自動化平台，其政策引擎涵蓋所有企業資產，能夠對所有資產進行持續的態勢評估。此外，Forescout 還提供允許網路存取策略的完整性監控。
企業收集盡可能多的有關資產、網絡基礎設施和通信現狀的信息，並利用這些信息來提升其安全態勢。	Forescout 收集的資訊遠超其政策引擎所使用的範圍；然而，Forescout 通過開放的 API 和雙向整合，將所有收集到的資訊提供給整個企業使用。

Forescout是 Zero Trust 架構的基礎元件

掌握設備Real-Time完整可視性並進行持續性合規驗證-依據當下可信任結果給予網路存取權限



LOCAL AGENT CENTRIC 連動裝Agent的資安工具	PERIMETER CENTRIC 連動邊界資安工具	ACCESS NETWORK CENTRIC 連動有線無線交換器	APPLICATION CENTRIC 連動應用層管理
vmware airwatch IBM MobileIron CROWDSTRIKE Carbon Black. FIREEYE McAfee Symantec.	paloalto NETWORKS Check Point SOFTWARE TECHNOLOGIES LTD. FORTINET.	NATIVE ACL & VLAN SUPPORT CISCO JUNIPER hp Alcatel-Lucent BROCADE MOTOROLA Aerohive Extreme networks LINKSYS CISCO TrustSec/SDA	vmware NSX amazon web services Microsoft Azure CISCO ACI illumio (OIM)

Reference: NIST 800-207

Forescout eyeFocus的設備攻擊面與暴露風險管理方法

- ▶ 一覽無遺的威脅動態儀錶板為管理層與資安團隊隨時掌握全院攻擊面與及合規安全狀態提供了堅實的基礎



全面網路資產管理(IT、IoT、IoMT、OT)

- ▶ 具持續跟進且準確的資產分類清單，可追蹤設備狀態和組態變更的歷史記錄，並搭配雲端AI引擎與威脅情資的智能風險分析，以幫助資安團隊利用資產情境內容和狀態趨勢來簡化操作

持續的資產風險情報

- ▶ 基於組態相關的網路暴露面指數與漏洞可利用率風險分析-獨特的多因素風險評估，其內容涵蓋IBM X-Force Exchange的EPSS威脅情資和CISA的KVE等主流威脅情資、評估暴露的服務(如開放端口、公共API或未加密的數據流不安全的通訊傳輸等)及弱安全態勢(如有重大問題的韌體版本或設備型號未更新修補或使用默認憑證等)。

物聯網安全性升級

- ▶ 透過無中斷的被動發現技術，利用高保真的物聯網分類以實現部署靈活性，即時識別泛物聯網漏洞，幫助安全團隊了解攻擊面並確定回應行動的優先順序

加速事件回應：

- ▶ 利用過去的資產情境內容來幫助資安分析師對風險進行主動調查，並對事件和事故做出反應，從而幫助盡量縮小攻擊範圍，縮短平均解決時間(MTTR)

Exposure Management Dashboard

TIMERANGE: Last 14 Days

Organisational Risk Score

7.4 High ↑ +13%

Risk Score Breakdown

- Confidence: 8%
- Posture: 10%
- Vulnerabilities: 47%
- Threats: 10%
- Internet Exposure: 5%

The Total Risk Score is calculated using Confidence, IT Posture, Open Ports, Threats and Vulnerabilities as Assessments. Check the Risk Score Breakdown for more detailed information.



Top Reasons for Risk

VULNERABILITY	DESCRIPTION	REMIEDIATION	CONFIDENCE	EXPLOITABILITY	CVSS	N. ASSETS	RISK REDUCTION
CVE-2022-000	Multiple Aruba switches buffer overflow	Update firmware	High	Extreme	9.8	32	22% ↓
CVE-2023-010	Juniper Networks Junos OS on EX Series and SRX Series	Apply latest security patch	High	Extreme	9.8	25	10% ↓
CVE-2023-001	Cross-Site Scripting (XSS) vulnerability in Hirschmann	Implement content security policy	High	Extreme	9.6	15	9% ↓
CVE-2023-002	Buffer overflow in Dell Server's network driver	Install driver updates	High	Extreme	9.6	12	9% ↓
CVE-2023-003	Improper access controls in GE Healthcare Ultrasound sy...	Restrict user privileges	High	Extreme	9.2	10	7% ↓
CVE-2023-004	Vulnerability in the firmware update mechanism of Cisco...	Use secure update protocols	High	Extreme	9.1	8	2% ↓
CVE-2023-005	Denial-of-service (DoS) vulnerability in Rockwell PLCs	Configure rate limiting	High	Extreme	9.1	6	2% ↓
CVE-2023-006	Privilege escalation vulnerability in HP Workstations	Patch operating system	High	High	8.6	4	1% ↓
CVE-2023-007	Security flaw in Philips MRI system	Update the system	High	High	8.5	2	1% ↓
CVE-2023-008	Insecure API implementation in Honeywell Smart Buildin...	Implement robust authentication	High	High	8.4	2	1% ↓

Top 5 Exposure Remediations

Change default access password Default Credentials	800 Assets	Risk Score Reduction	22% ↓
Apply recommended patches CVE-2017-11892	400 Assets	Risk Score Reduction	18% ↓
Implement network segmentation CVE-2018-11776	278 Assets	Risk Score Reduction	15% ↓
Use encrypted protocol Insecure Authentication Method	200 Assets	Risk Score Reduction	7% ↓
Block communications to comprom... Potential Threats Communications	12 Assets	Risk Score Reduction	2% ↓



VULNERABILITY	DESCRIPTION	REMIEDIATION	CONFIDENCE	EXPLOITABILITY	CVSS	N. ASSETS	RISK REDUCTION
CVE-2022-000	Multiple Aruba switches buffer overflow	Update firmware	High	Extreme	9.8	32	22% ↓
CVE-2023-010	Juniper Networks Junos OS on EX Series and SRX Series	Apply latest security patch	High	Extreme	9.8	25	10% ↓
CVE-2023-001	Cross-Site Scripting (XSS) vulnerability in Hirschmann	Implement content security policy	High	Extreme	9.6	15	9% ↓
CVE-2023-002	Buffer overflow in Dell Server's network driver	Install driver updates	High	Extreme	9.5	12	9% ↓
CVE-2023-003	Improper access controls in GE Healthcare Ultrasound sy...	Restrict user privileges	High	Extreme	9.3	10	7% ↓
CVE-2023-004	Vulnerability in the firmware update mechanism of Cisco...	Use secure update protocols	High	Extreme	9.2	8	2% ↓
CVE-2023-005	Denial-of-service (DoS) vulnerability in Rockwell PLCs	Configure rate limiting	High	Extreme	9.1	6	2% ↓
CVE-2023-006	Privilege escalation vulnerability in HP Workstations	Patch operating system	High	High	8.6	4	1% ↓
CVE-2023-007	Security flaw in Philips MRI system	Update the system	High	High	8.5	2	1% ↓
CVE-2023-008	Insecure API implementation in Honeywell Smart Buildin...	Implement robust authentication	High	High	8.4	2	1% ↓

Forescout eyeFocus AI風險分析引擎能自動分析和量化每個IP連接設備的風險嚴重性及可利用性

- ✓ 顯示當下企業「總風險分數」以及「各設備各別風險分數」
- ✓ 顯示當前網路安全狀態的即時概覽，以快速識別高風險區域、脆弱系統和潛在威脅
- ✓ 提供風險狀態的趨勢圖以利管理階層檢視安全投資和修復行動的影響，瞭解網路安全狀態是改善還是惡化？
- ✓ 讓用戶知道最快速跟合適風險修復與緩解措施
- ✓ 「各設備造成風險的主要原因」並提供可行的破口修復建議或風險緩解措施，以指導有效的資源配置並以最具有成本效益的方式降低風險。

ForeScout eyeFocus 量化設備風險嚴重等級並提供緩解建議

FORESCOUT CLOUD Reza ? [→]

Exposure Management ? TIME RANGE Last 14 Days ▼

DEVICE CATEGORY: All ▼ VENDOR: All ▼ FUNCTION: All ▼

Top Reasons For Risk

[Vulnerabilities](#) [Posture](#) [Compliance](#)

VULNERABILITY	DESCRIPTION	REMEDIATION	EXPLOITABILITY	CVSS	N. ASSE...
CVE-2017-0145	Microsoft Server Message Block version 1 code execution	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	8.1	16
CVE-2017-0144	Microsoft Server Message Block version 1 code execution	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	8.1	16
CVE-2017-0146	Microsoft Server Message Block version 1 code execution	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	8.1	16
CVE-2017-0148	Microsoft Server Message Block version 1 code execution	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	8.1	16
CVE-2017-0143	Microsoft Server Message Block version 1 code execution	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	8.1	16
CVE-2019-12255	Wind River VxWorks TCP Urgent Pointer buffer overflow	The WindRiver advisory provides more information about the vulnerabilities and p...	● Critical	9.8	10
CVE-2017-0147	Microsoft Server Message Block version 1 information disclo...	Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin...	● Critical	5.9	16
CVE-2019-12257	Wind River VxWorks DHCP buffer overflow	The WindRiver advisory provides more information about the vulnerabilities and p...	● Critical	8.8	10
CVE-2017-3881	Cisco IOS and Cisco IOS XE CMP code execution	Refer to Cisco Security Advisory cisco-sa-20170317-cmp for patch, upgrade or su...	● Critical	9.8	6
CVE-2018-0171	Cisco IOS and Cisco IOS XE Smart Install buffer overflow	Refer to Cisco Security Advisory cisco-sa-20180328-smi2 for patch, upgrade or su...	● Critical	9.8	6
CVE-2017-6738	Cisco IOS and IOS XE Software remote code execution	Refer to Cisco Security Advisory cisco-sa-20170629-snmpp for patch, upgrade or s...	● Critical	8.8	6
CVE-2018-0167	Cisco IOS, IOS XE, and IOS XR Software Link Layer Discov...	Refer to Cisco Security Advisory cisco-sa-20180328-ldp for patch, upgrade or sug...	● Critical	8.8	6
CVE-2018-0174	Cisco IOS and IOS XE Software DHCP option 82 encapsula...	Refer to Cisco Security Advisory cisco-sa-20180328-dhcpr3 for patch, upgrade or ...	● Critical	8.6	6

Forescout eyeFocus設備合規與組態狀態變化的跟蹤

The screenshot displays the Forescout eyeFocus interface, showing a detailed view of a device's communication flow. The main window is titled "vs-ad-001.demofs.com" and displays a "Communication Flow" diagram. The diagram shows a central node labeled "10.100.44.98" with multiple blue lines representing communication paths to various other devices. The devices are listed on both the "Inbound" and "Outbound" sides, including "ct-2654 (computer)" and "ct-7620 (server)".

On the left side, there is a sidebar with several sections:

- Exposure**: Includes a filter and organization information.
- Device Overview**: Shows a "Total Risk Score" of 9.4 and a "Device Status Over Time" chart.
- Top Reasons**: Lists vulnerability findings, including CVE-2023-201.
- Configuration Findings**: Lists configuration issues.
- Top Five Device Actions**: Lists actions such as "Device Action", "Policy Update", "Firmware Upgrade", "Device Reboot", and "New Device Onboarding".

The main window also includes a header with the Forescout logo, user information (Demo-Account, David), and a search bar. The device details section shows a "Risk Score" of 9.4 and a "Risk Severity" of Critical. The communication flow diagram is a Sankey-style flow chart showing data flow between devices.

設備風險評估與回應措施決策

持續性評估設備風險

了解設備的風險有助於優先處理並評估應對措施

有兩種方法可以確定風險：

- 自我評估定義的風險
- 由Forescout計算風險

Forescout 的零信任政策引擎允許您將風險管理納入自動化工作流程中，以採取相應的行動。這種方法能依據設備的風險指數，執行不同層次的應對措施，從而提高安全性和效率



透過明確的風險指數決定事件處理順序並優化對事件和威脅的回應時間與效率

不僅執行風險告警並可透由零政策管理引擎驅動自動化風險回應流程

Before Forescout: 完全仰賴人力處理風險，常常緩不濟急或會錯失最佳處理時機



Automated Cyber Security Workflows

After Forescout: 加入零信任策略管控能進行依據過往事件處理經驗設置預防性自動化風險回應管理



01 Align Risk to Assets

每個IP連接的數位資產的風險評分都與 Forescout eyeFocus即時共享，以套用於 Forescout eyeSight的資安政策管理引擎

02 Prioritize Response

透過 Forescout 整體平台的治理能力，利用獨特的風險指數來確定設備風險處理的優先等級與緊急程度

03 Optimize Remediation

減少警報疲勞並根據預設的Forescout政策管理引擎腳本驅動eyeControl進行風險減緩措施或自動修復action，使資安團隊人員能專注在更需要人力研讀或判斷處理的事件上

Zero Trust: Policy Orchestration 運用協同進行聯合防禦

政策



Data Center



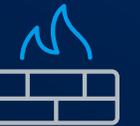
Centralized Network



Campus



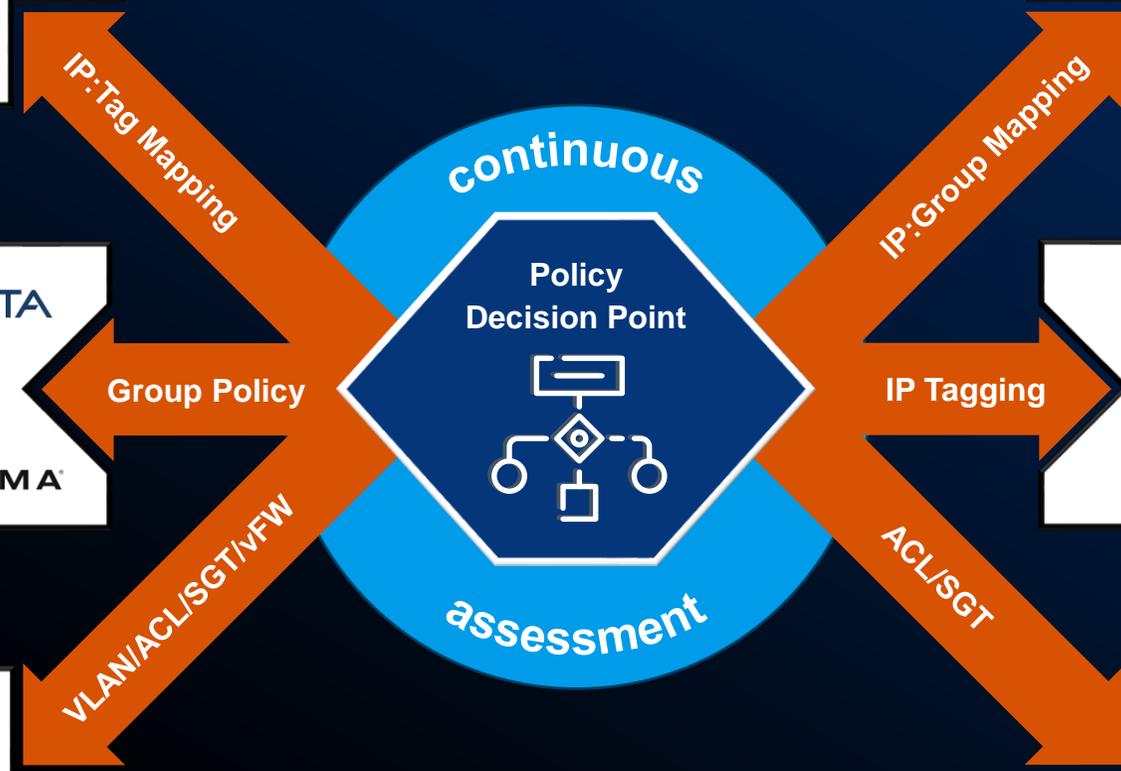
Cloud



Firewall



VPN



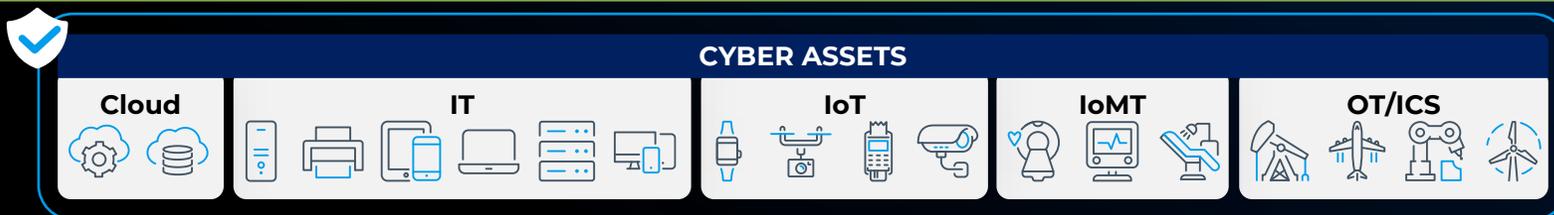
ForeScout 幫你打造支援多廠牌的單一統籌自動化平台



FORESCOUT PLATFORM

持續的即時發現並確保組織內所有數位資產的安全能維持各層面的合規

Predictive
↑
Proactive
↑
Reactive



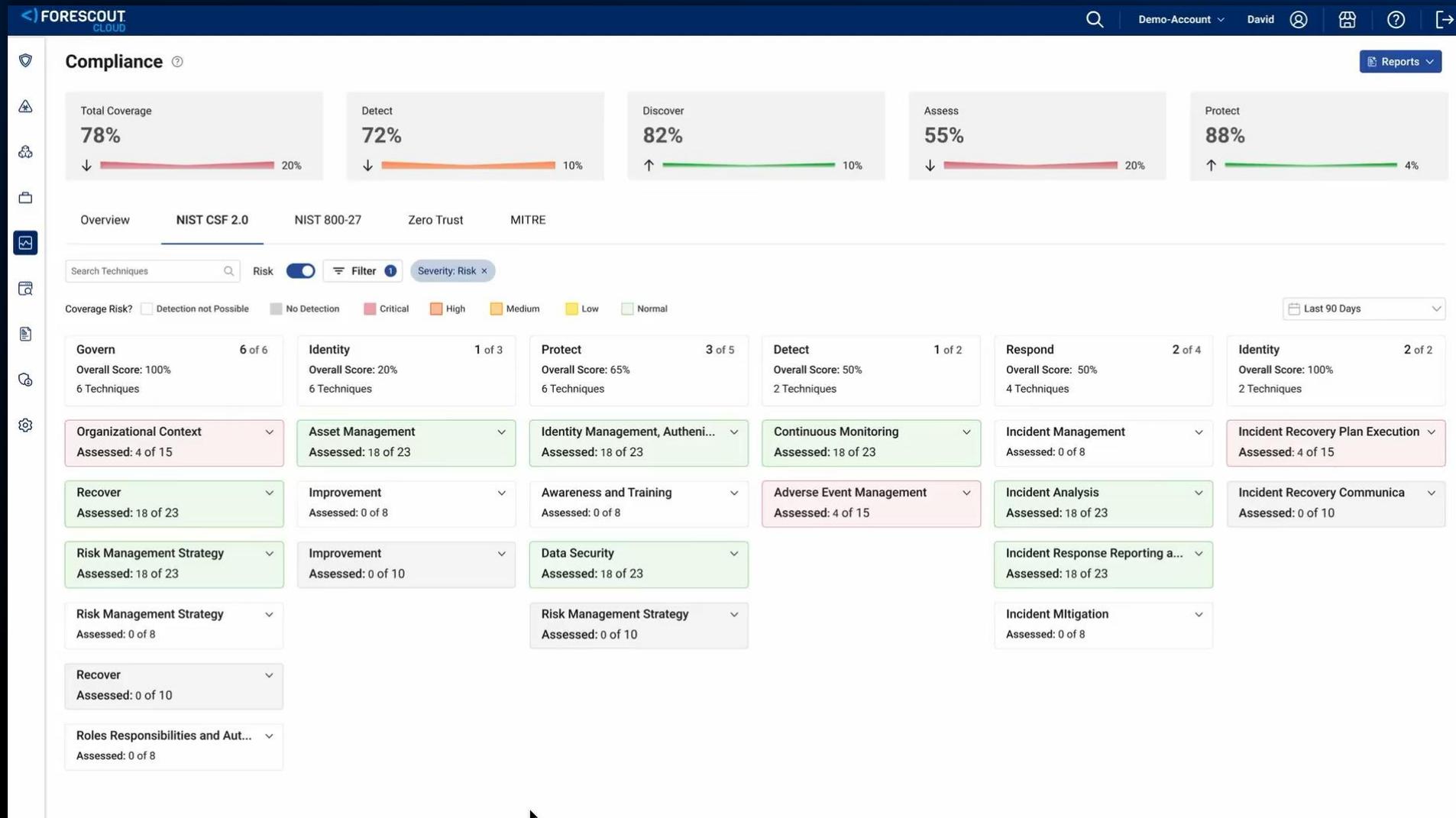
將國際安全框架整合進Fore Scout 4D Platform™簡化了合規管理流程



Forescout 平台能自動將合規政策對應到CSF2.0的安全控制框架

NIST CSF 2.0

- 識別控制細節
- 展示缺口
- 需優先處理下一步
- 用豐富的上下文屬性
- 識別可執行的步驟
- 以達成網路安全成果



Thank you.

<) FORESCOUT

