

揭開黑暗之處的光明燈： 用完整可視能力治理隱藏在暗處的威脅

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



2024已知漏洞被利用研究報告-by Forescout Vedere Labs資安研究室

漏洞被發現、武器化和利用的速度比以往任何時候都還要快!

2023年有97個零日漏洞被利用(VL-KEV)。2024 年開始到五月的零日漏洞數量已達到 31 個

- ✓ 近九萬個漏洞沒有 CVE ID，而且這個數字每年都在增加
- ✓ 2023 年發現了超過 21,200 個未分配 CVE ID 的問題
 - 到 2023 年，沒有 CVE ID 的漏洞比 2021 年增加62%
- ✓ 44% 沒有 CVE ID 的漏洞可用於取得系統存取權限
 - 37% 的嚴重程度為High或Critical
 - 45 個被利用的漏洞沒有 CVE ID (佔總數的 2.15%)
- ✓ 四個漏洞資料庫中(CISA KEV、AttackerKB、Shadowserver、VL-KEV)總共發現了 2,087 個不同的被利用漏洞：
 - 沒有一個資料庫能夠單獨包含所有訊息
 - CISA KEV包含的被利用漏洞總數1055個(佔50%)
 - 968個漏洞僅出現在一個資料庫(佔47%)
 - 90個漏洞出現在四個資料庫 (佔4%)

Devices Affected by VL-KEV Vulnerabilities Not on CISA

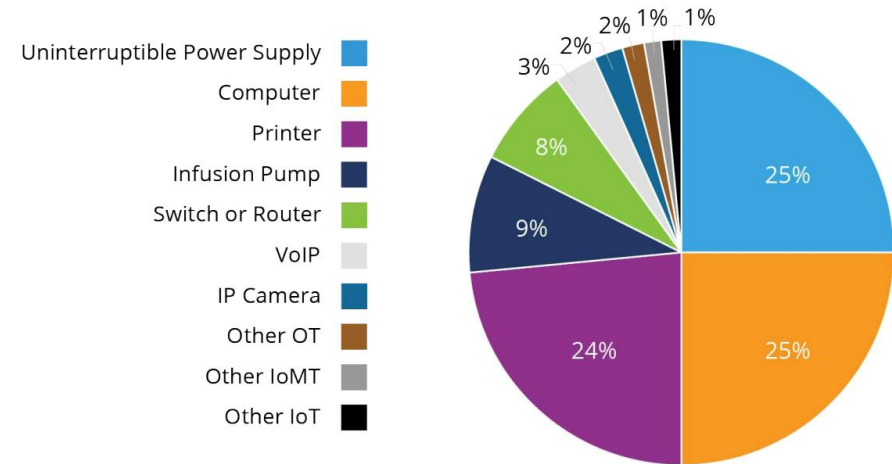


Figure 6 – Devices on customer networks affected by VL-KEV vulnerabilities not on CISA

企業要能即時有效地實施風險緩解，需要有一種能力：

- ◆ 自動辨識易受攻擊網路上的資產(不能單看CVSS漏洞指標)
- ◆ 辨識目前被利用的問題(如果服務沒開,有漏洞也不會是風險)
- ◆ 自動了解這些資產可能容易受到攻擊的環境(辨識能成功的條件)

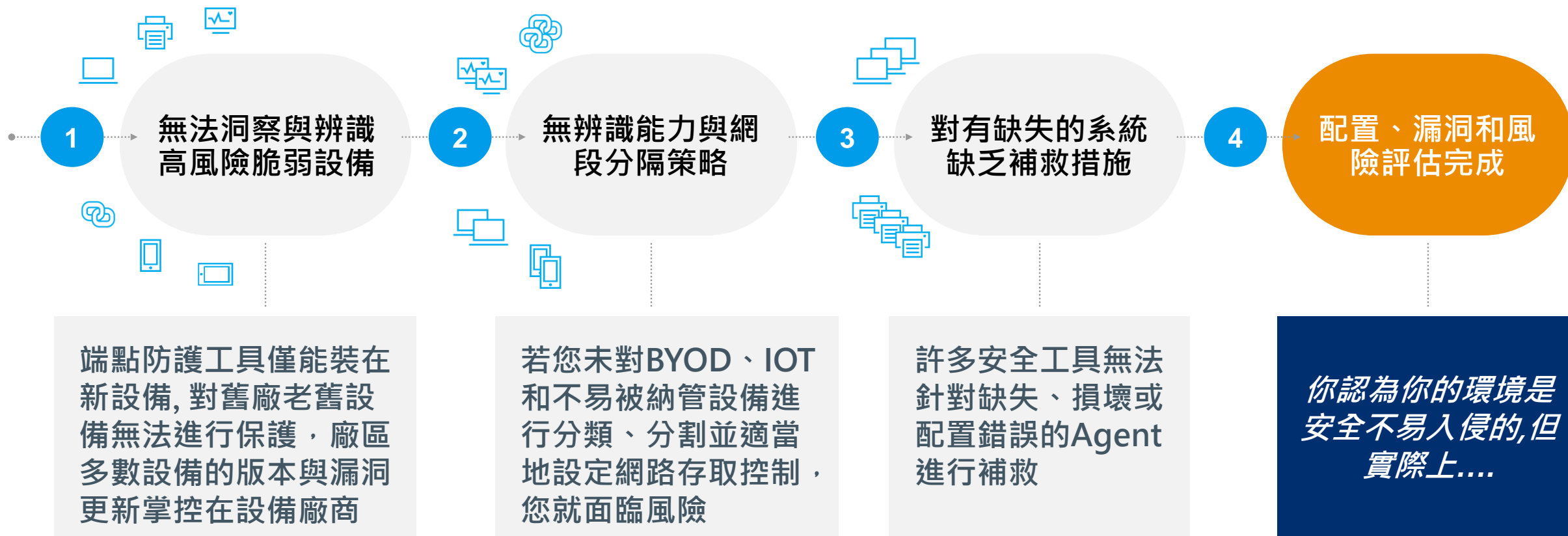
備註說明:

CISA KEV - CISA Known Exploited Vulnerabilities Catalog

VL-KEV- Forescout Known Exploited Vulnerabilities Catalog

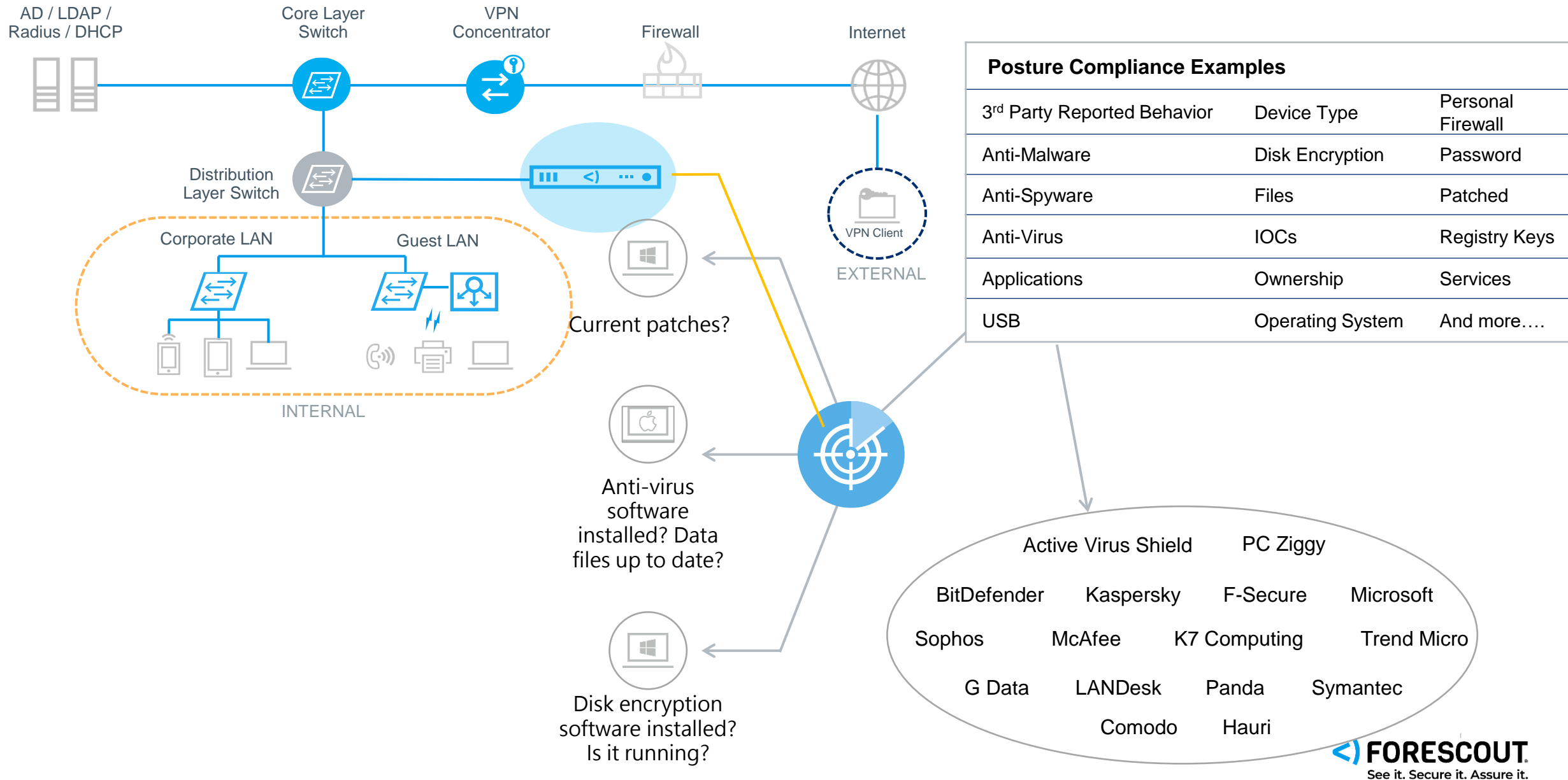
針對易受攻擊的高風險脆弱設備,無採取適當風險減緩措施,導致入侵機會擴大

這些年,那些已投資主流資安工具確還遭受勒索攻擊成功的受災戶之共同點



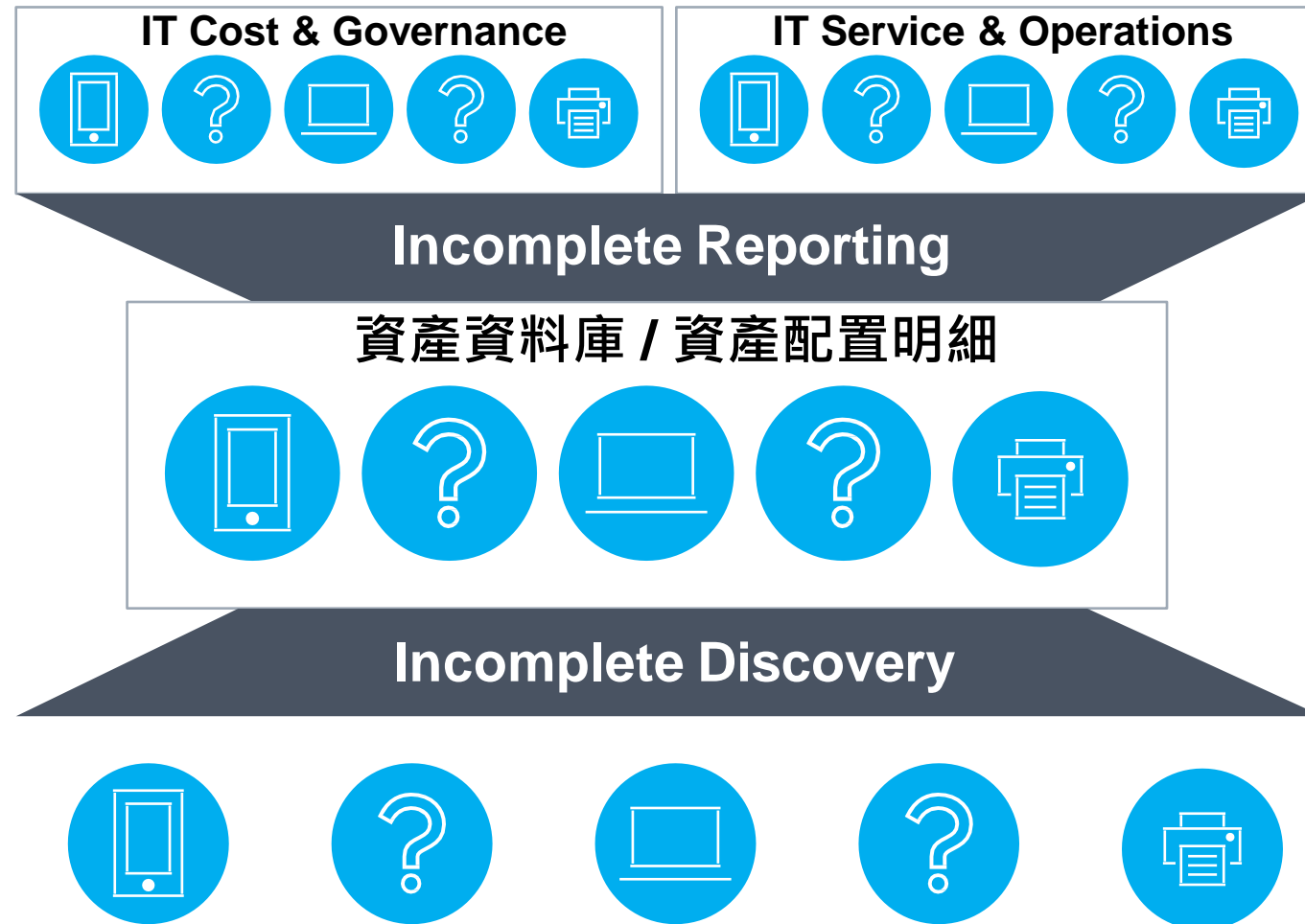
設備沒管好伴隨的就是更多網路風險

合規就是為了管好設備,預先做好避免風險



完整設備可視性是治理設備風險的成功基石

Poor Data Input = Poor Data Output



Forescout透由整合的力量即時發現並識別與感知設備與網路的變化

Continuous asset discovery and profiling

The Forescout platform yields rich data about a variety of endpoints (IT, IoT and OT) without requiring software agents or previous device knowledge.

WHO ARE YOU?

- Employee
- Partner
- Contractor
- Guest

WHO OWNS YOUR DEVICE?

- Corporate
- BYOD
- Rogue

WHAT TYPE OF DEVICE?

- Windows, Mac
- iOS, Android
- Virtual machine
- Non-user devices, IoT, OT

WHERE/HOW ARE YOU CONNECTING?

- Switch/Port/PoE
- Wireless/Controller
- VPN
- IP, MAC
- VLAN

WHAT IS THE DEVICE HYGIENE?

- Configuration
- Software
- Services
- Patches
- Security Agent

And More

Forescout從根源取得最真實可信的設備即時資訊作為檢測條件

認證屬性 / AD 屬性

憑證、HTTP Login、
AD User、Group...

分類 / 高級分類屬性

功能、OS、廠商/型號、網
路功能、Service Banner...

設備資訊

IP、Label、合規、網域、介
面、腳本結果...

事件屬性

設備上線、設備離線、ARP
Spoofing、**惡意事件**、C/S 會話...

Windows 屬性

NetBIOS成員資訊、OS、
檔案、登錄用戶...

Windows 應用屬性

運行的程序、服務...

Windows 安全屬性

防毒軟體狀態、Windows
Patch更新狀態...

屬性變化跟蹤

用戶名、文件
大小等

Linux / Mac 相關屬性

主機名稱、腳本結果、檔、
管理狀態、程序、使用者...

外設相關屬性

Name、ID、Class、USB 類
型、狀態、

SNMP/交換機屬性

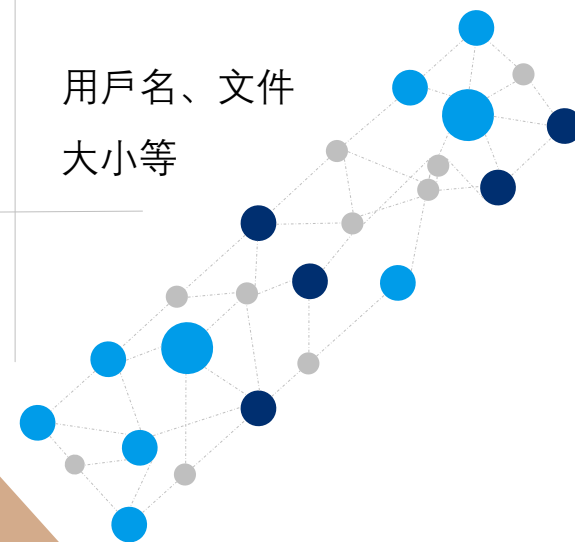
SNMP MIB值、交換機埠、
VLAN、ACL、POE...

訪客註冊

核准狀態、核准人、註冊狀
態、註冊資訊...

遠端可管理性屬性

MS-RRP / MS-SMB / MS-
WMI 可管理性



by Forescout整合偵測引擎

Foreshout資產可視性的細緻度 - 硬體CPU、RAM、HDD、製造商.... 等等

HWI-Computer

Host	IPv4 Address	Segment	Policy HWI-
WORKGROUPIT14-...	192.168.65.1	Foreshout-Training	HWI-Com

HWI-Computer

Profile Compliance All Policies

**User:** chad (local) **IPv4 Address:** 192.168.65.1 **Hostname:** T14-PF2ZDST7 **Operating System:** Windows 10 Professional
MAC Address: 005056c00008 **Domain:** WORKGROUP **Function:** Workstation
Vendor and Model: VMware

Matched the [HWI-Computer](#) policy on June 28 01:36:07 PM [View policy flow](#)


Match Main Rule

Condition Properties: Computer:

Name:	+ T14
User Name:	+ T14
Primary Owner Contact:	+
Primary Owner Name:	+ Cha
Support Contact Description:	+
Part Of Domain:	+ No
Domain:	+ WO
Domain Role:	+ Star
Workgroup:	+ WO
Roles:	+ LM_
Manufacturer:	+ LEN
Model:	+ 20W
OEM String Array:	+
Description:	+ ATIA
Caption:	+ T14
System Type:	+ X64
PC System Type:	+ Mob
Current Time Zone:	+ GMT
Bootup State:	+ Norr
Number Of Processors:	+ 1
Total Physical Memory (Megabytes):	+ 324
Keyboard Password Status:	+ Not
Power Management Supported:	+

HWI-Physical Memory

Profile Compliance All Policies

**User:** chad (local) **IPv4 Address:** 192.168.65.1 **Hostname:** T14-PF2ZDST7 **Operating System:** Windows 10 Professional
MAC Address: 005056c00008 **Domain:** WORKGROUP **Function:** Workstation
Vendor and Model: VMware

Matched the [HWI-Physical Memory](#) policy on June 28 01:45:25 PM [View policy flow](#)

Match Main Rule

Condition Properties: Physical Memory:

Name:	+ 實體記憶體
Caption:	+ 實體記憶體
Description:	+ 實體記憶體
Manufacturer:	+ Crucial Technology
Removable:	+
Replaceable:	+
SKU:	+
Part Number:	+ CT16G4SFRA32A.M16FRS
Serial Number:	+ E53A071F
Other Identifying Info:	+
Status:	+
Capacity:	+ 17179869184
Memory Type:	+ Unknown
Data Width:	+ 64
Bank Label:	+ BANK 0
Device Locator:	+ Controller1-ChannelA-DIMM0
Speed:	+ 3200
Name:	+ 實體記憶體
Caption:	+ 實體記憶體
Description:	+ 實體記憶體
Manufacturer:	+ Samsung
Removable:	+
Replaceable:	+
SKU:	+
Part Number:	+ M471A2G44AM0-CWE

Forescout資產可視性如何能準確落實合規機審計？

Views

Search

Policies

Compliance

Corporate/Guests

1.1 (Primary) Classification (24)

CrowdStrike Visibility Beyond Campus (0)

Linux設備密碼原則檢查 (1)

符合企業規範 (1)

不符合企業規範 (0)

Monitor Managed Switches (0)

Filters

Search

All

Segments (24)

Organizational Units

Default Groups

Groups

端點IT設備合規檢測

法規要求檢查描述

伺服器系統要啟動作業系統自動安全更新

開啟複雜性密碼設定

設定密碼最長使用期限：90天

設定帳戶鎖定閾值：5次

設定帳戶鎖定時間：15分鐘(含)以上。

設定限制密碼最小長度：8碼。

設定密碼歷程記錄：3

設定重設帳戶鎖定計數器的時間間隔：15分鐘

伺服器系統須安裝防毒軟體及設定自動更新病毒碼。

設定連線階段逾時(SessionTimeout)設定，即登入後，超過15分鐘沒有活動即應由系統自動強迫登出。

設定定時與TimerServer矯正系統時間。

1 OF 24 HOSTS

Policy Linux設備...

Function

Actions

are Virtual Machine

符合企業規範

Server

符合企業規範

Profile

Compliance

All Policies

IPv4 Address: 192.168.40.224

Operating System: Ubuntu 22.04

MAC Address: 000c29cf0728

Function: Server

Vendor and Model: VMware Virtual Machine

1. Match 符合企業規範

Condition Properties: Linux_Pass_Status:

PASS_MAX: 99999

PASS_MIN: 0

TMOUT: 1200

minlen: 33

retry: 8

remember: 4

Actions: None (No actions defined for this rule)

The host is not inspected by the remaining sub-rules because it matches 符合企業規範

2. N/A 不符合企業規範

取得設備密碼有效期限(天數)

兩次更換密碼的最小週期(天數)

Session連線活動

密碼輸入錯誤次數

密碼幾代相同

See it. Secure it. Assure it.

Forescout 合規檢測能涵括Linux、MAC OSX、Windows

1.3.0 Overall Compliance

1.1. Discovery

1.3.1 Windows

1.3.2 MAC OSX

1.3.3 Linux

1.3.3.1 Cybereason

1.3.3.2 Landesk for Linux

Landesk exception

Landesk Installed

Landesk Not Installed

1.3.3.3 Malwarebytes

1.3.3.4 Symantec

1.3.3.5 Linux IT Center

1.3.4 SC Agent

1.4 Informational

1.3.3.1 Cybereason for Linux

Search

Host	IPv4 Addr...	Segment	Policy 1.3.3.1 Cybereason for Linux	MAC Add...
WORKGROU...	10.106.226...	CNSHA06-wir...	Cybereason Installed for Linux	94c69180f...
WORKGROU...	10.33.52.139	BRVCP01-wir...	Cybereason Not Running for Linux	e41f13ec8...
WORKGROU...	10.5.12.96	CNSZX01-wir...	Cybereason Not Running for Linux	e04f43e60...
MYGROU\P...	10.104.3.81	CNHUI01-wired	Cybereason Not Running for Linux	0894ef5aa...
LENOVO.CO...	10.36.50.64	USWHI01-wir...	Cybereason Installed for Linux	0800279d...
100.65.247.169	100.65.247...	ZIN63-wireless	Cybereason Installed for Linux	f48c50bfbf...
10.99.24.97	10.99.24.97	CNPEK06-wir...	Cybereason Not Running for Linux	ecd68a8d...
10.99.24.39	10.99.24.39	CNPEK06-wir...	Cybereason Not Running for Linux	000c2979...

FORESCOUT
See it. Secure it. Assure it.

透過Fore Scout智慧政策引擎進行檢測及控管- 自動化策略設計

Name

NameLinux設備密碼原則檢查

Edit

Description

None.

Scope

IP RangesAll IPv6,All IPv4

Edit

Filter by Group

None.

Exceptions

None.

Main Rule

Conditions	Actions	Re-check Matched
IPv4 Address: 192.168....		Every 8 hours, All admis...

Edit

Sub-Rules

Name	Conditions	Actions	Exceptions
1 符合企業規範	Linux_Pass_Stat...		
2 不符合企業規範	NOT Linux_Pass...		

Add

Edit

Remove

Duplicate

Up

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	符合企業規範	Linux_Pass_Stat...		
2	不符合企業規範	NOT Linux_Pass...		

Add

Edit

Remove

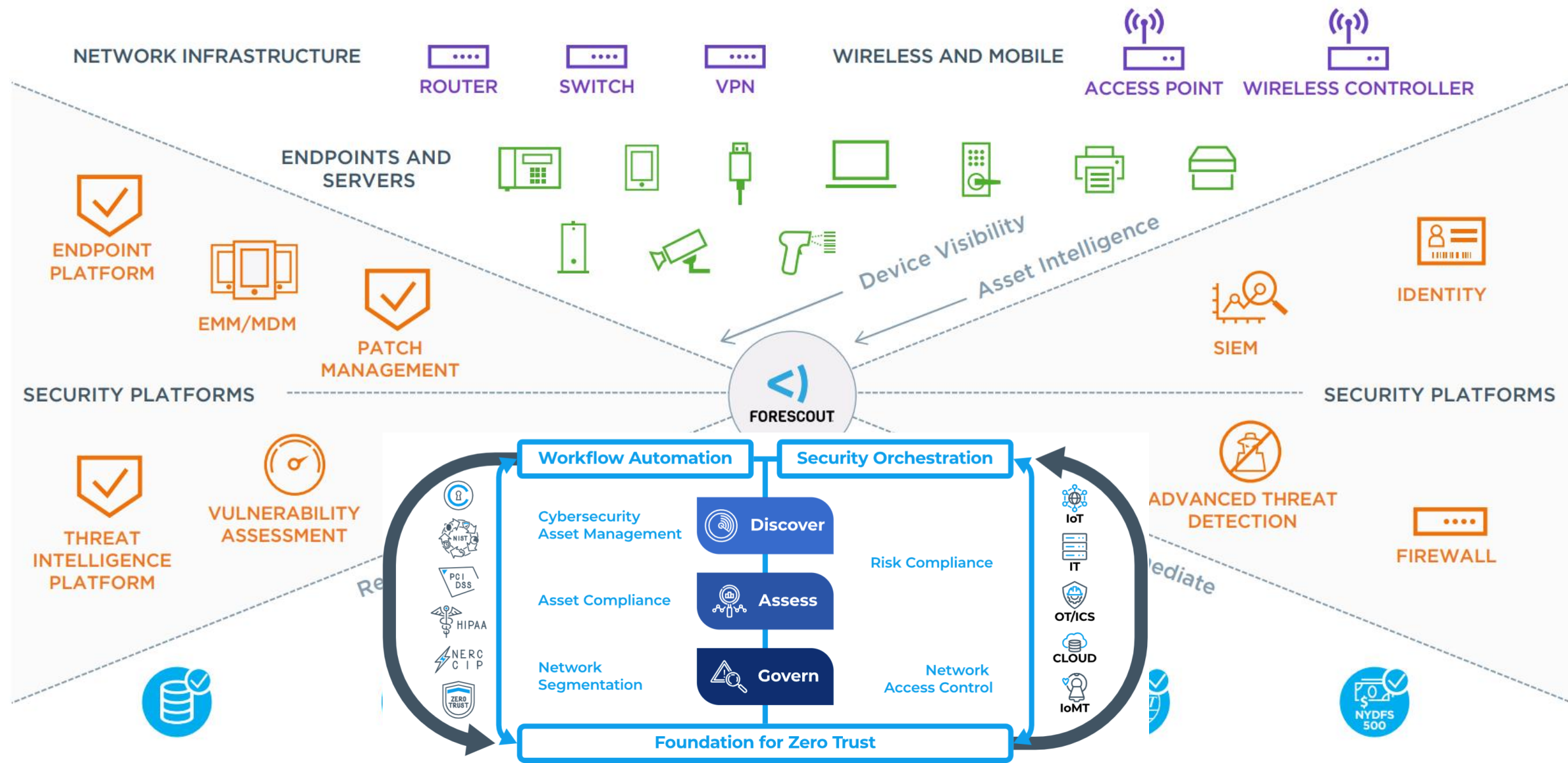
Duplicate

Up

資產可視性與安全基準線合規狀態



Forescout具備即插即用整合模組,輕易將你的環境轉變為持續合規管理的零信任資安架構



AI浪潮來襲，資安團隊如何跟上要求？



83%

of cybersecurity personnel feel
overworked

資安人員過勞是常態!



Where to
focus?

眼前該關注那些?



How to
prioritize?

那些該先著急?



What to
protect?

該保護那些脆弱的?

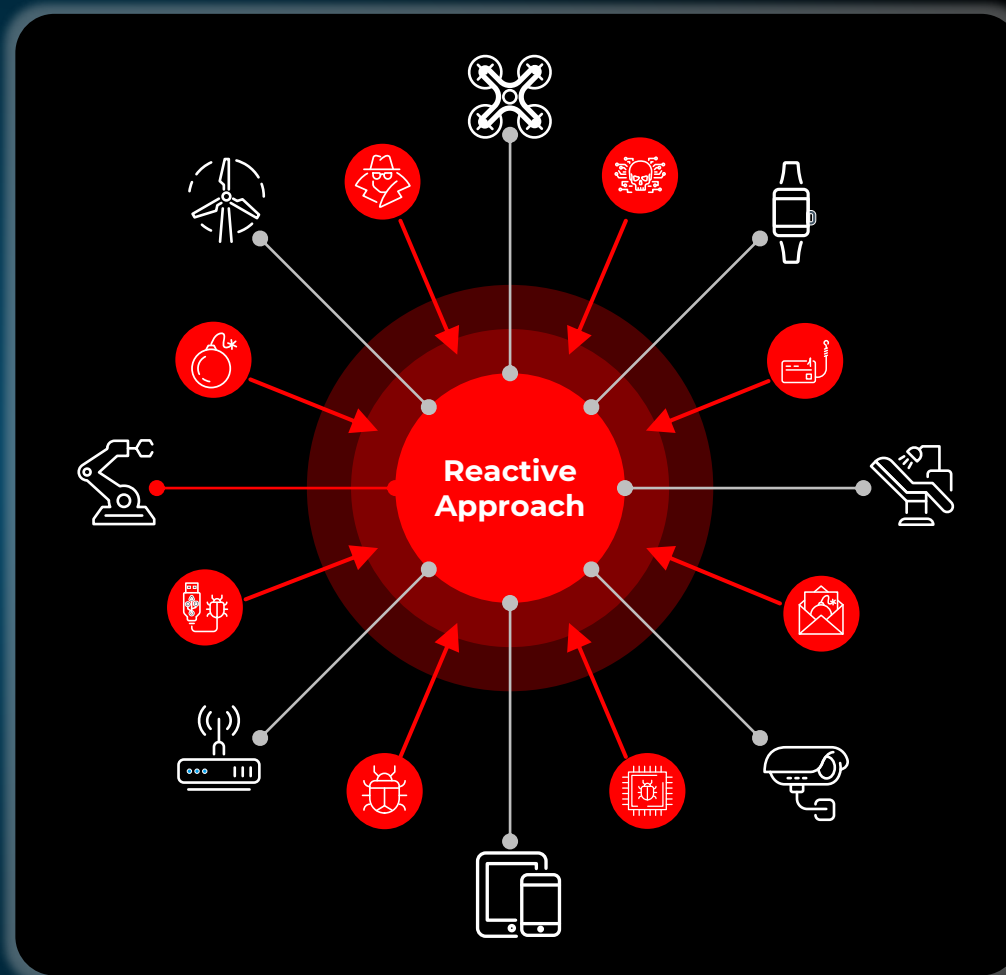
傳統的方式已跟不上駭客進化的速度!

A Reactive Security Approach is **Not Enough**

傳統被動回應式解決方案(Reactive Solutions):

- ▶ 使用太多的工具來防禦一切
- ▶ 變得複雜、昂貴且資源密集
- ▶ 在整合和資料共享方面產生問題

... and create more
HEADACHES
for the security teams



Focus on What Matters Most : Cyber Risk

- ▶ 關注業務需求,提供對關鍵風險的更好洞察力
- ▶ 透過預防而非事後處理,因此可以節省成本。
- ▶ 能夠區分出噪音和真正的威脅,聚焦在最薄弱的環節

SIMPLIFIED EXPERIENCE

for the security teams

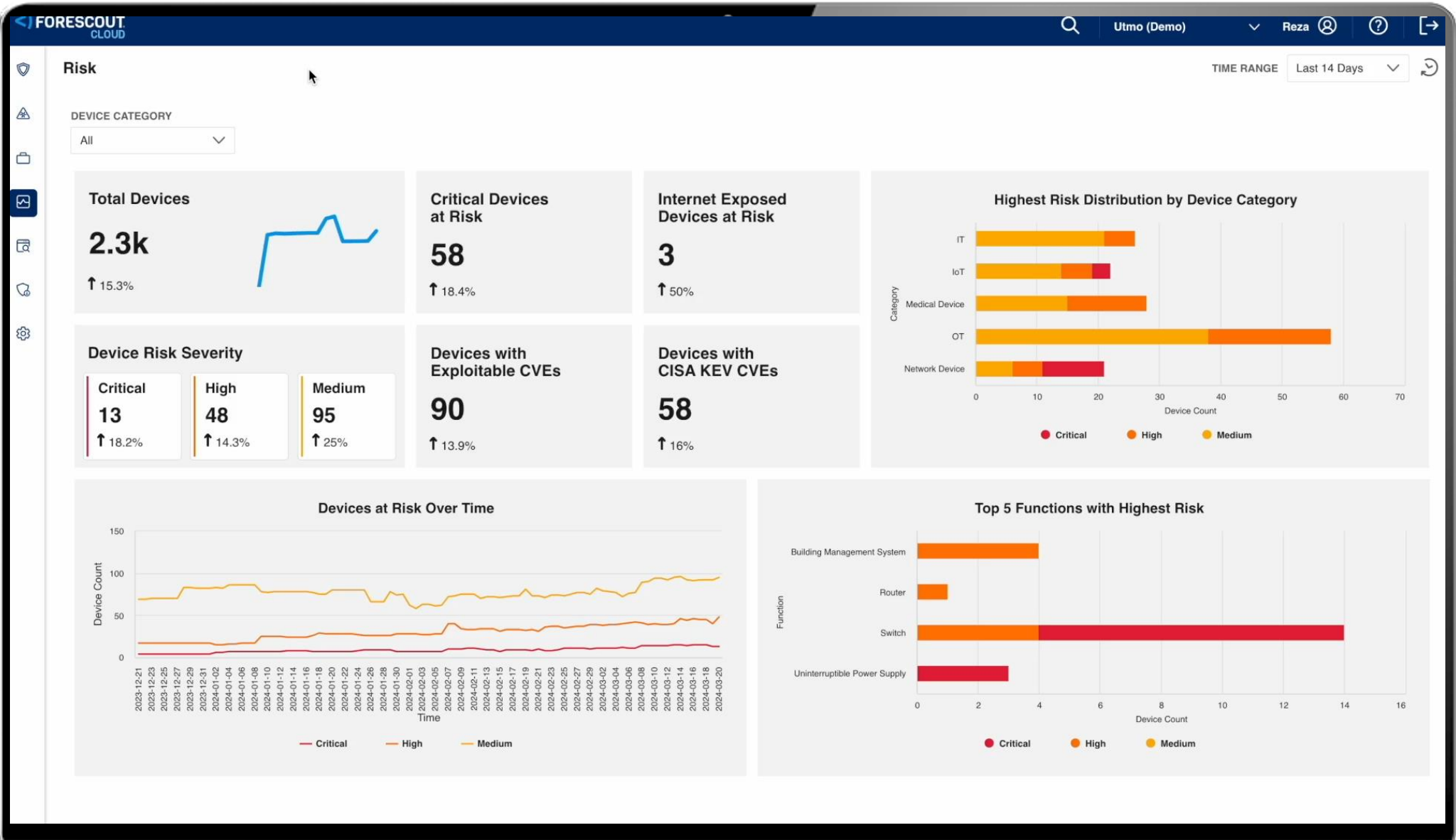


長官與資安治理人員的視野

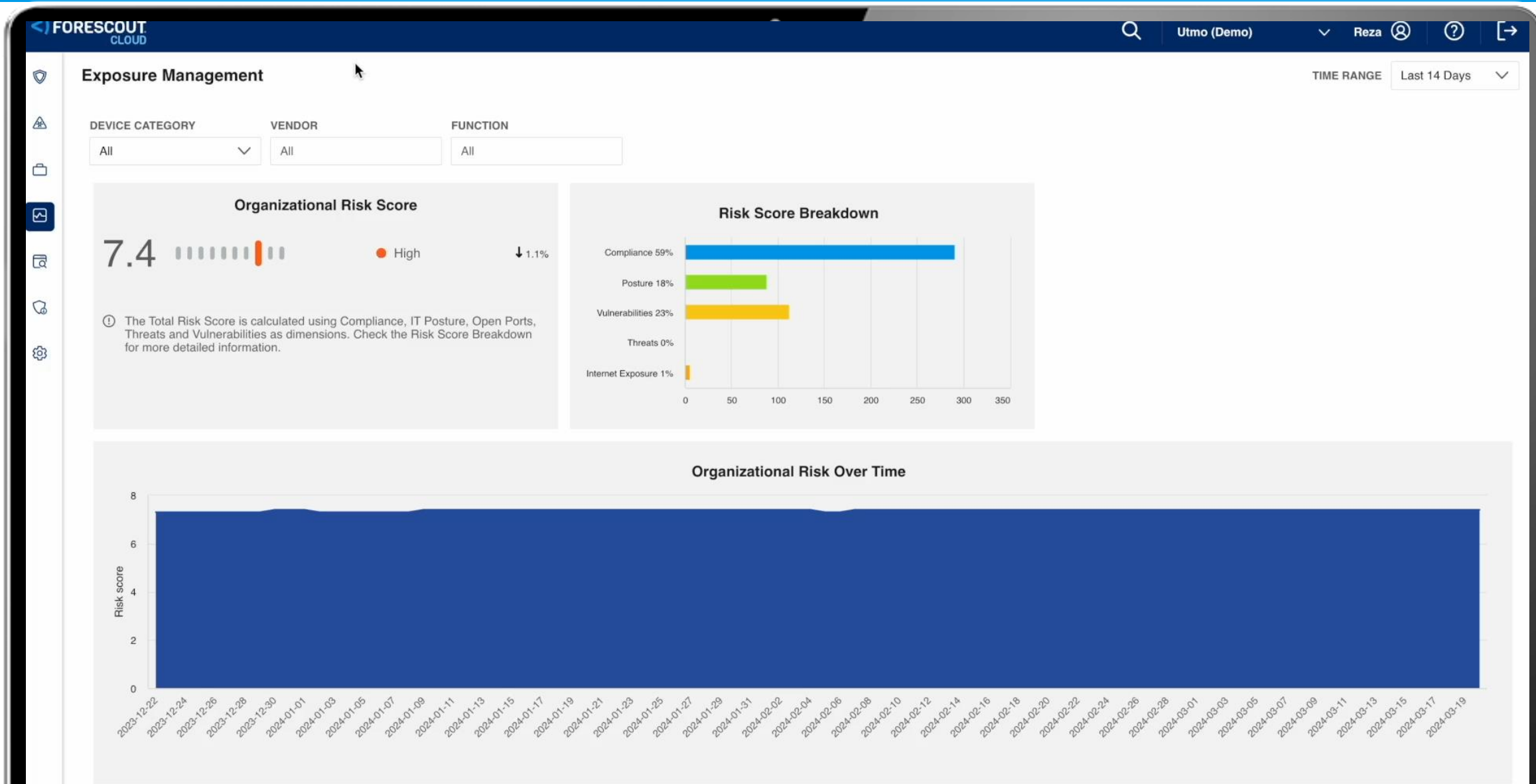
那些沒有管好 vs 已經管了那些



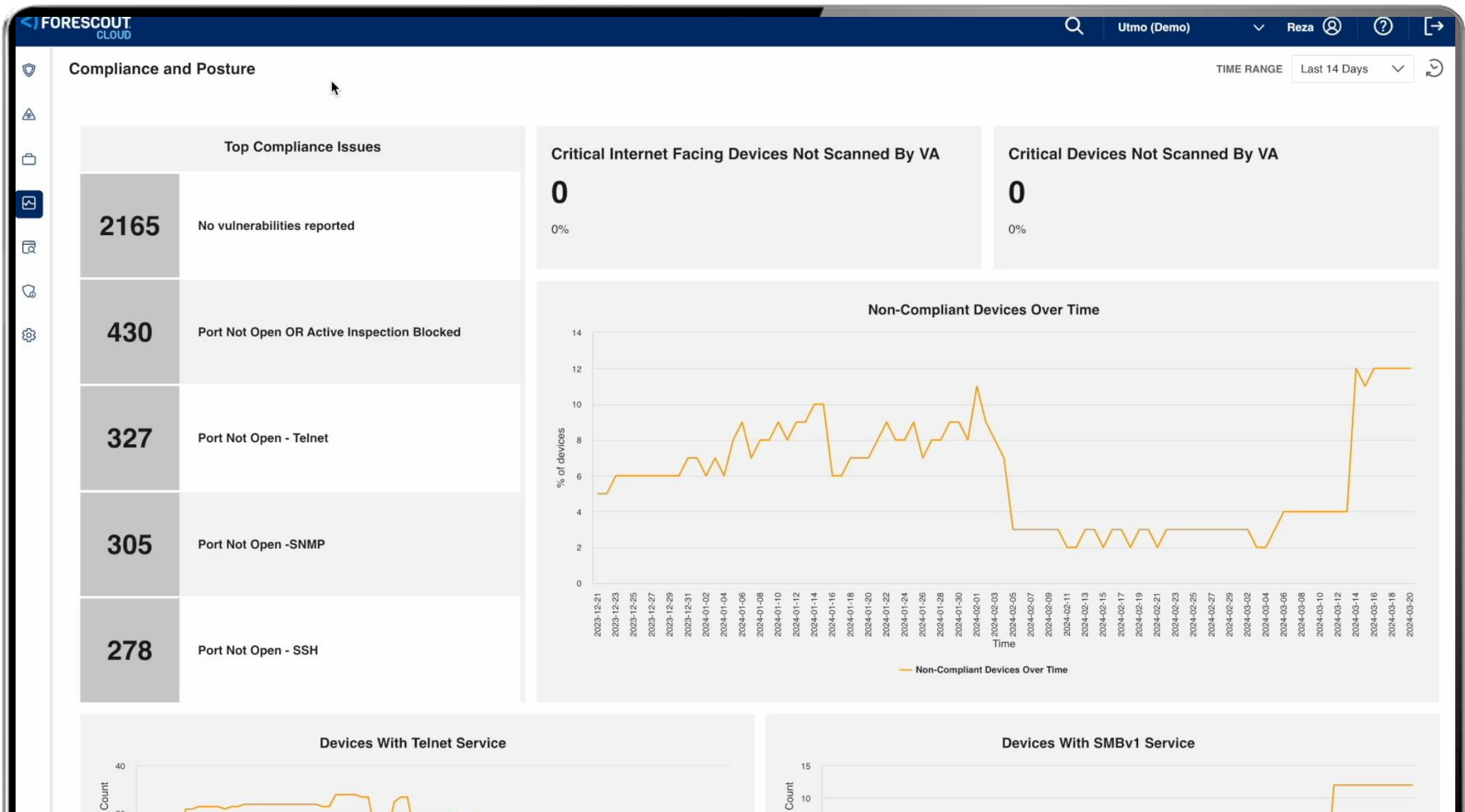
Forescout 量化風險讓團隊做出更好的決策



有效地強化企業管理風險態勢,提升對潛在風險的應對能力



更輕鬆能達成合規審計的要求

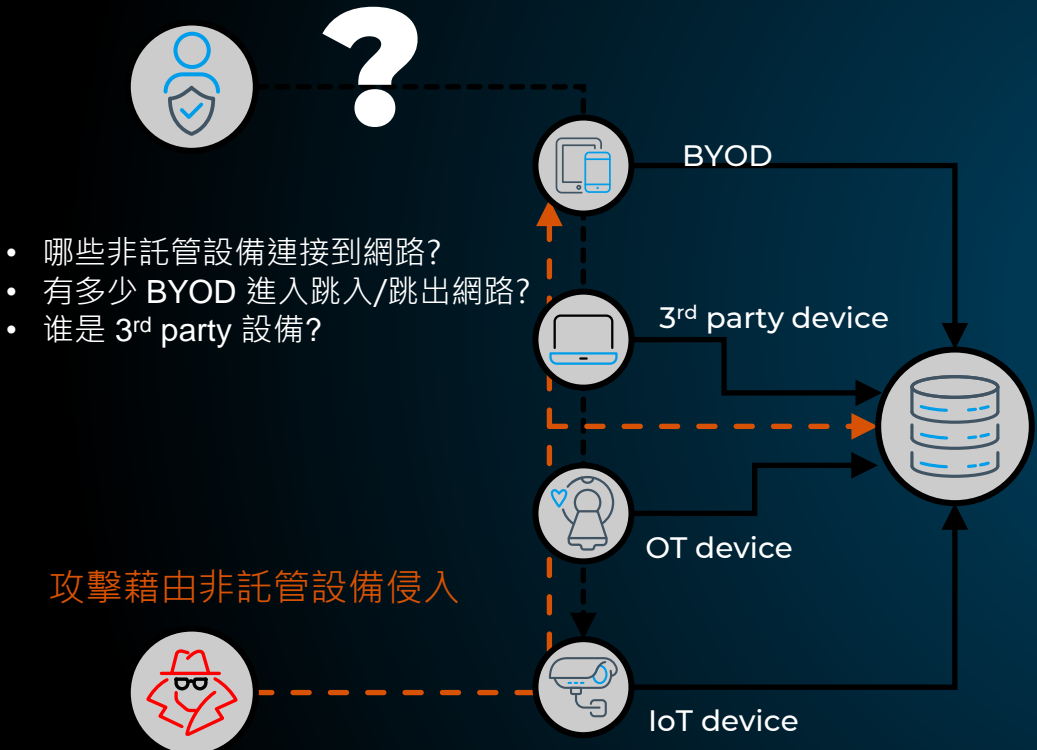


實務場景1: See it – Comprehensive Visibility

BEFORE
FORESCOUT

Simplify
Experience

AFTER
FORESCOUT

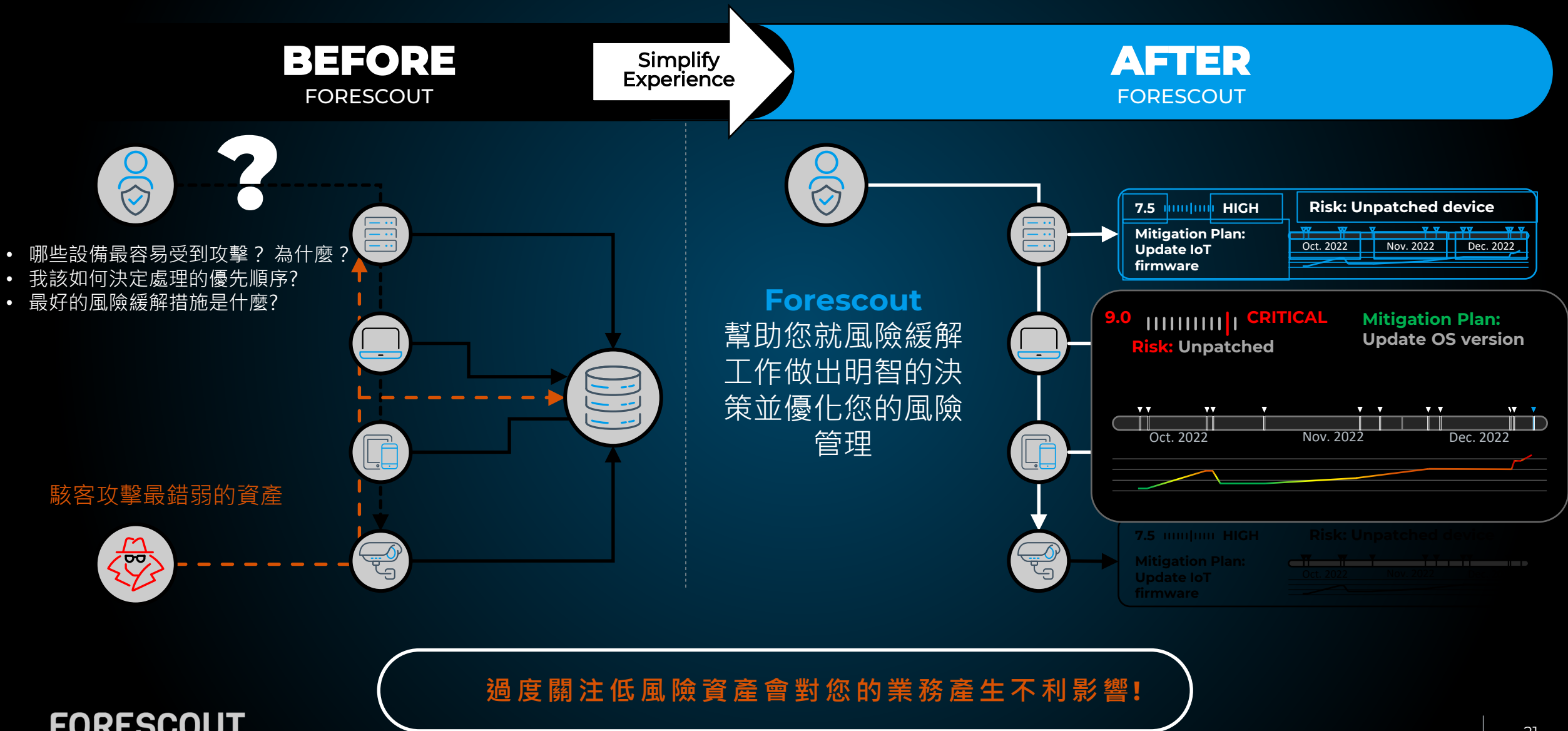


Forescout
幫助您輕鬆識別非託
管設備及其暴露屬性，
實現即時感知您設備
真實風險變化

Category: Medical Device Function: MRI Scanner Vendor: Siemens Model: Magnetom MRI	OS: Windows IP Add: 10.100.28.10 Port: 370 / UDP Recall: 20 Oct. 2020
Category: 3rd Party Device	OS: Windows 10
Category: Medical Device Function: MRI Scanner Vendor: Siemens Model: Magnetom MRI	OS: Windows IP Add: 10.100.28.10 Port: 370 / UDP Recall: 20 Oct. 2020

Visibility is always a TOP priority,
because you can protect what you can't see!

實務場景2 : Secure it – Business Continuity



實務場景3: Assure it – Compliance Readiness

BEFORE
FORESCOUT

Simplify
Experience

AFTER
FORESCOUT



漏洞評估

滲透測試

安全政策審查

存取權限評估

身分管理評估

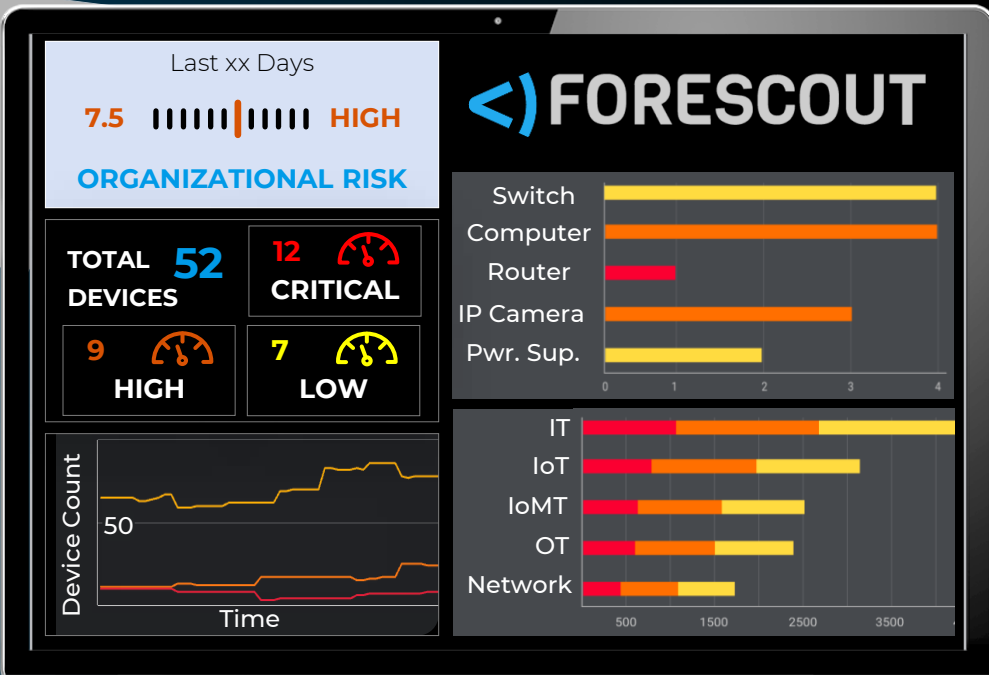
漏洞更新評估

And
More

- 用於合規落差分析的工具太零散無效率！
- 如何理解從不同工具得到的數據？
- 一個持續且永無止境的過程



Forescout
持續評估和主動式
矯正強化企業的安全態勢，以確保合
規審計輕鬆過關



FORESCOUT

立即獲得掌握存在企業內的風險與合規狀態的完整洞察力！

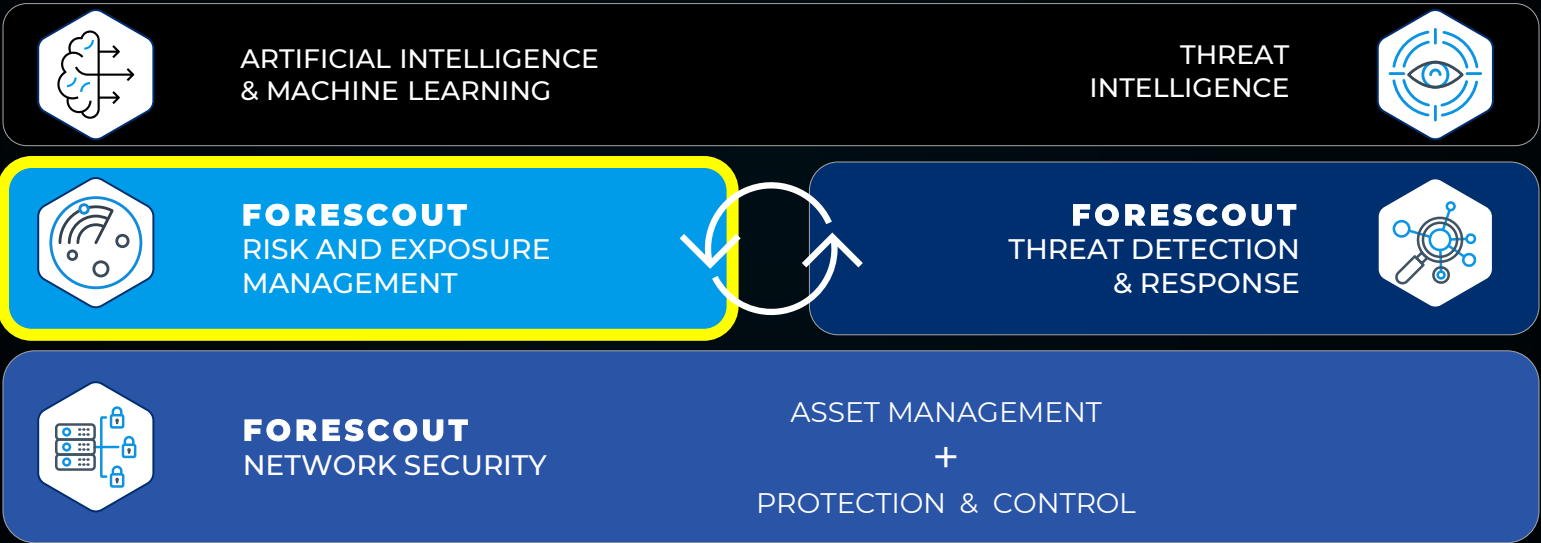
Forescout幫你打造支援多廠牌的統籌自動化平台



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



運用Forescout整合與自動化智慧引擎 打造強大聯合自動防護框架&逐步簡化資安維運成本與重複投入

資安框架目標

在我的網路存在那些設備？ 這些設備帶來哪些脆弱點及易受攻擊面的風險？ 甚麼已經穿透我的防護網變成須處理的威脅？ 該如何處理這些威脅進行即刻修補與風險回應？以及調整那些合規管理策略預防未來？

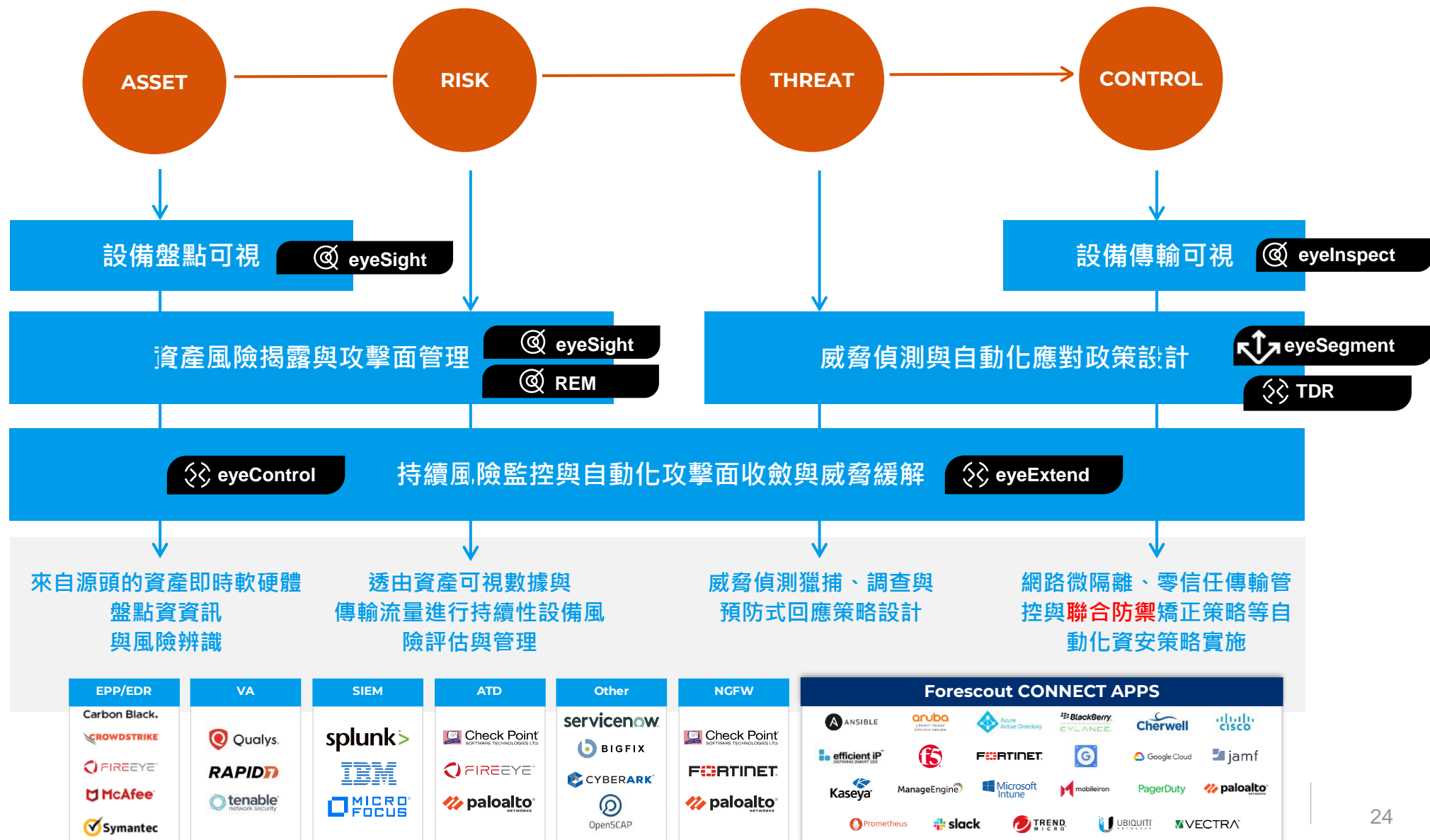
< FORESCOUT

Cybersecurity Asset Management

Network Security & Threat Security

Workflow Automation

Security Orchestration



Forescout AI 透由可信的數據為你簡化所有煩人的作業



<) FORESCOUT.

攤位:P206

Thank you.

<) FORESCOUT[®]
See it. Secure it. Assure it.



5/15 (三)

14:45 - 15:15

7F | 701G

人工智慧與假訊息的新世代

Rik Ferguson

Forescout
Vice President Security Intelligence, CTO Office

今年我們很榮幸地邀請到 Forescout 國際知名的資安專家 Rik Ferguson，他將與我們一同分享國際最新的威脅資訊，為資安界點亮一盞明燈。Rik Ferguson 是 Forescout 安全情報副總裁，全球網路安全領域的領先專家，擁有超過 25 年的資安經驗，是資安界的明星人物之一。他的演講風格深受人們喜愛，屢獲殊榮，是您不容錯過的資安權威。

最新訊息
馬上得

活動 1

Rik Ferguson
Meet & Greet

5/15 Day 2 | 13:30-14:00

在攤位分享 Forescout 資安研究室 Vedere Labs 現下最急迫的漏洞威脅，及其對全球帶來的影響。與全球資安明星 Rik Ferguson 面對面交流，分享經驗。

與全球資安明星 Rik Ferguson
持 Forescout 手燈拍立得合照

我也有
明燈

活動 2

Forescout 攤位明星禮

參加以上二者任一活動即可獲得 Forescout
攤位明星禮一份

豪禮
1+1

典藏 - 丹麥手沖咖啡全套組
(活動每日抽出一位)

除可獲得攤位明星禮以外，並於每日活動結束前抽出一位幸運參加者，
贈送 Forescout 典藏「丹麥手沖咖啡全套組」(價值TWD\$4000)。



<) FORESCOUT[®]
See it. Secure it. Assure it.