EXTRAHOP

運用NDR網路可視性實現零信任整合

林孟忠

ExtraHop North Asia

Sam Lin

Sr. Sales Engineer

公司簡介

- 2007年成立於美國西雅圖
- 2015年在新加坡設立亞太總部
- 創辦人Jesse Rothstein & Raja Mukerji 來自 F5 Networks 的資深系統架構師
- Gartner MQ 與 EMA Radar 領導者
- 全球頂尖企業及政府單位所信任的網路Visibility,偵測與分析的平台
- 全球一千多客戶, 一萬多部屬，保護1000多萬的重要資產 (critical asset)
- 業界機器學習及進階分析的創新者

ExtraHop Named a Leader in The Forrester Wave™:

Network Analysis And Visibility, Q2 2023

> “Commands the market with its depth and breadth of enterprise features.”
>
> “Large enterprises with hybrid and multicloud deployments should evaluate ExtraHop.”

LEADER

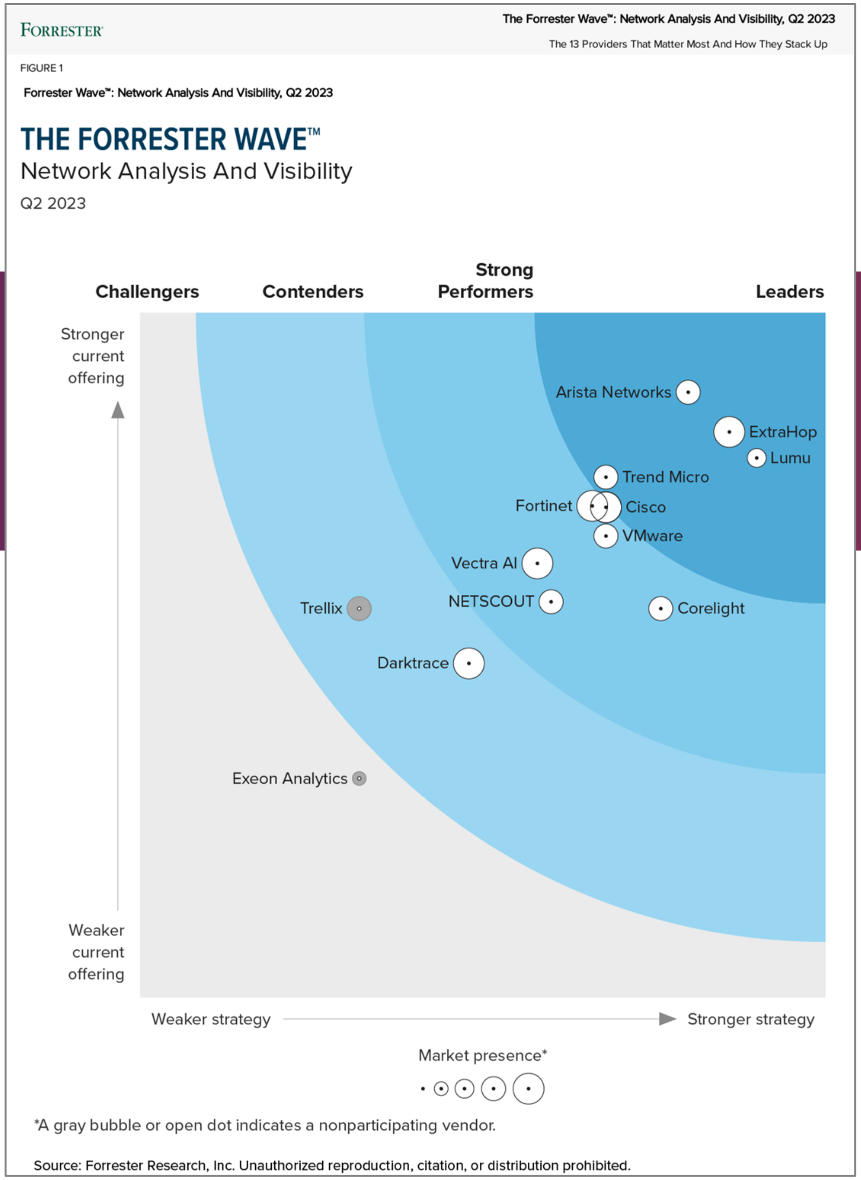
ExtraHop’s ability to decrypt all traffic, including TLS 1.3 and PFS, provides deep insight into all packets and the payloads they contain.

ExtraHop’s superior vision focuses on exposing assets that touch the network without introducing additional overhead and noise that require a heavy lift from SOC analysts.

The UI is intuitive and easy to navigate, providing contextual breakdowns of what’s happening and why it’s important.

IT also gives robust MITRE ATT&CK correlation and the ability to drill down without having to open multiple consoles.

“Reference customers described ExtraHop relationship as being built on ‘mutual trust’ with a ‘focus on customer enablement’”



FORRESTER

The Forrester Wave™: Network Analysis And Visibility, Q2 2023

The 13 Providers That Matter Most And How They Stack Up

FIGURE 1

Forrester Wave™: Network Analysis And Visibility, Q2 2023

THE FORRESTER WAVE™

Network Analysis And Visibility

Q2 2023

*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

“NAV is a Critical Zero Trust Technology”

ExtraHop Analyst Coverage & Industry Recognition

Strategic Alignment with Leading Industry Firms

Gartner

Gartner Peer Insights Customers' Choice 2023 Industry

2023 Gartner® Peer Insights™
Customers Choice 2023

*ExtraHop earns distinction in Gartner® Peer Insights **Voice of the Customer for NDR***

Forrester

ExtraHop Network Analysis & Visibility Technology Recognized by Independent Research Firm

The Forrester NAV Landscape, 1Q 2023 acknowledges network visibility is fundamental to zero trust

Momentum Leader
WINTER
2024

CYBERSECURITY BREAKTHROUGH AWARD 2023
CLOUD BASED NETWORK SECURITY SOLUTION OF THE YEAR

Gartner

2022 Gartner® Market Guide for Network Detection & Response

ExtraHop is a Representative Vendor for the Third Time

Forrester

Forrester TEI Found 87% Reduction in Time to Resolve Threats with ExtraHop

**Study Concludes ExtraHop Reveal(x) 360 delivers cost savings & business benefits for enterprise customers*

RevealX was named Best AI-Based Solution for Cybersecurity in the AI Breakthrough Awards

CYBERSECURITY BREAKTHROUGH AWARD 2023

網路的可視性

建立零性任的基礎和管理網路風險

威脅行為者利用漏洞並不斷更改 TTP 以逃避偵測並擴大影響

70%
的網路流量已
加密

37%
的組織關鍵
設備不受管理

47%
的關鍵設備 **暴露在公共互聯網上**

98%
的組織運行一種或多種**不安全的網路協議**

現有的資安方案足夠嗎？

EDR
無法覆蓋所有的端點，
網路行為無法偵測

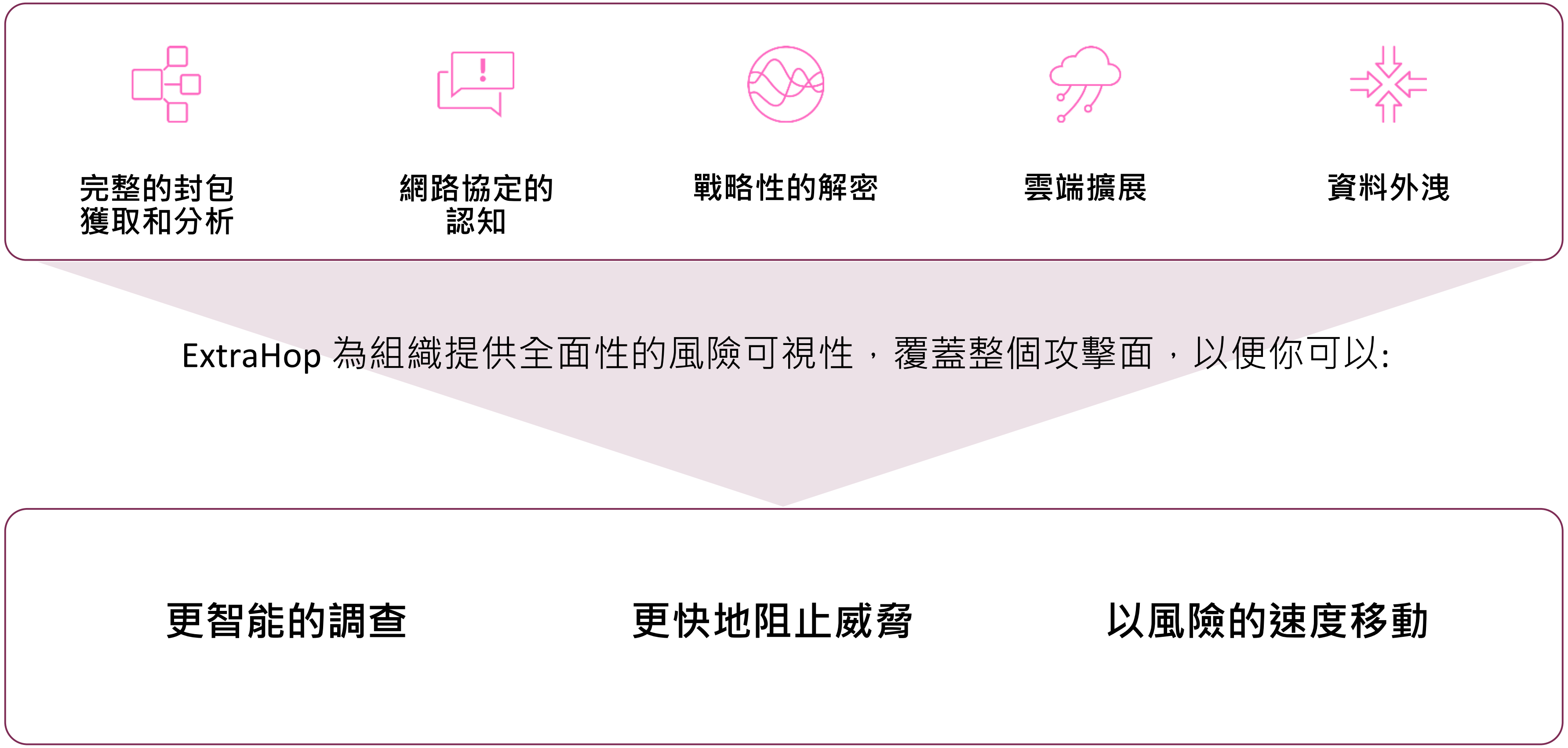
SIEM
不是用於專門偵測攻擊，
且日誌可以被Disable

IDS
只能偵測已知威脅

NGFW
缺乏東西向流量偵測，數據難
以納入調查工作流程

網路可視性來降低內部網路風險

RevealX 看見其他資安工具看不見的



技術 差異性

- 完整的封包獲取和分析
- 網路協定的認知
- 戰略性的解密
- 雲端擴展
- 資料外洩

ExtraHop 為組織提供全面性的風險可視性，覆蓋整個攻擊面，以便你可以:

商業 & 網路安全成果

- 更智能的調查
- 更快地阻止威脅
- 以風險的速度移動

Network Data is a Record of Ground Truth

ExtraHop Stream Processing and AI Models Extract the Actionable Insights

HTTP INTEL

- 121.35.232.13 □ 192.168.1.3:80
- http://www.extrahop.com/login
- 35s response time – **95% server delay**
- **500 server error**
- SessionID: ACD53332
- Cookie: ….
- UserName: john_smith
- OrderID: 3838383
- User agent: Firefox53/Windows10

SMB/CIFS INTEL

- User: \\WORKGROUP\jsmith
- File: \\WS1\Desktop\ **a.ppt.encrypted**
- Method: WRITE
- Access Time: 520 ms
- Network Transfer Time: 10 s
- Bytes Transferred: 500 MB
- UserName: john_smith

DATABASE INTEL

- 192.168.23.5 □ 192.168.25.8:1521
- User: **sa**
- Query: select * from accounts
- 20s response time – **90% server delay**
- Bytes Transferred: 100 KB
- Network Transfer Time: 0.5 ms
- Error: **ORA-00942 table or view does not exist**

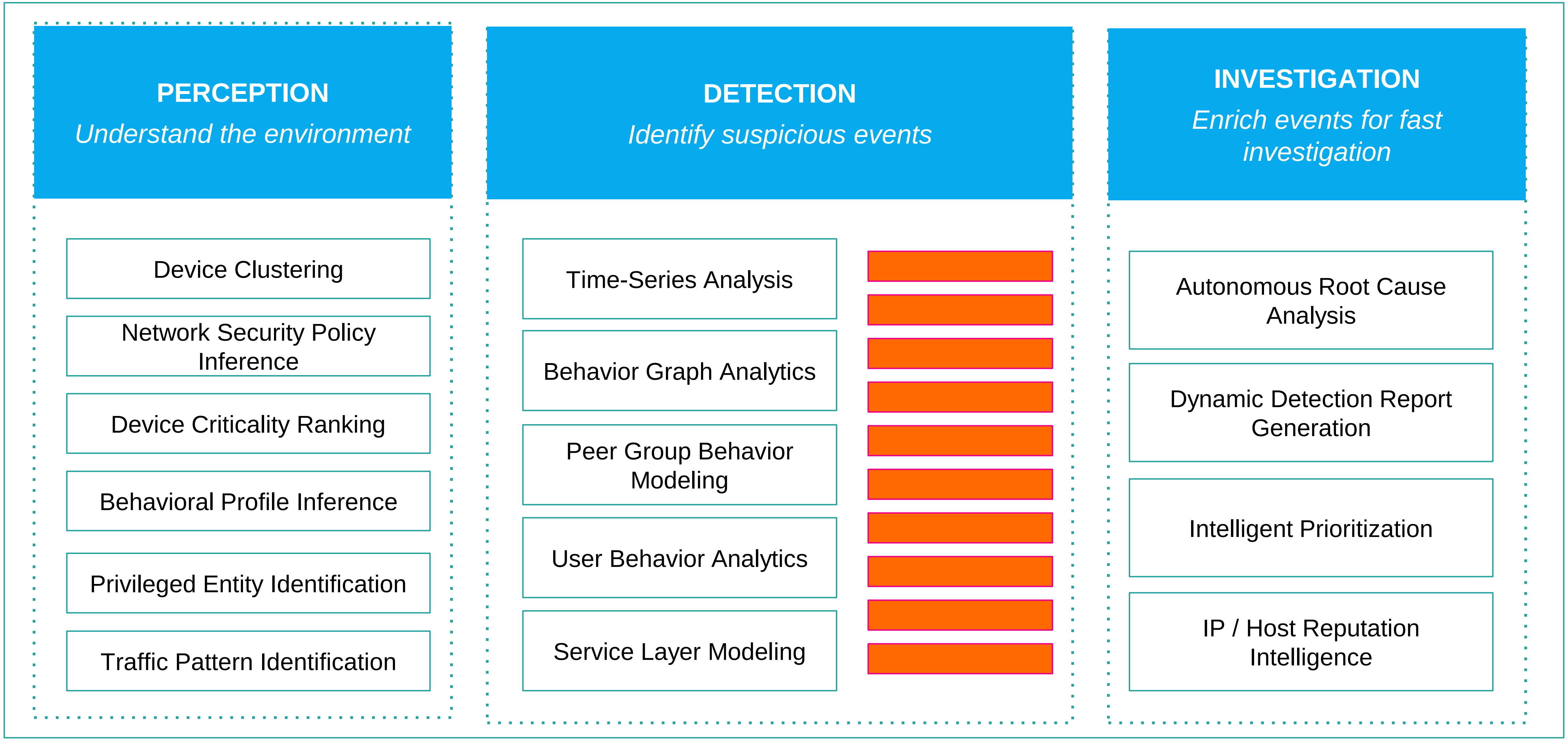
KERBEROS INTEL

- 192.168.23.2 □ 10.1.3.5:88
- User: ptdaniels
- Message Type: TGS Request
- Server Realm: sa.local
- 20 ms response time
- Bytes Transferred: 119 B
- Network Transfer Time: 0.5 ms
- Error: **KDC_ERR_CLIENT_REVOKED**

RevealX’s ML is Composed of Three Subsystems

□ *Modules*

🟧 *Detectors*



PERCEPTION

Understand the environment

- Device Clustering
- Network Security Policy Inference
- Device Criticality Ranking
- Behavioral Profile Inference
- Privileged Entity Identification
- Traffic Pattern Identification

DETECTION

Identify suspicious events

- Time-Series Analysis
- Behavior Graph Analytics
- Peer Group Behavior Modeling
- User Behavior Analytics
- Service Layer Modeling

INVESTIGATION

Enrich events for fast investigation

- Autonomous Root Cause Analysis
- Dynamic Detection Report Generation
- Intelligent Prioritization
- IP / Host Reputation Intelligence

領先MITRE ATT&CK 覆蓋率

更廣泛地覆蓋能降低風險的暴露

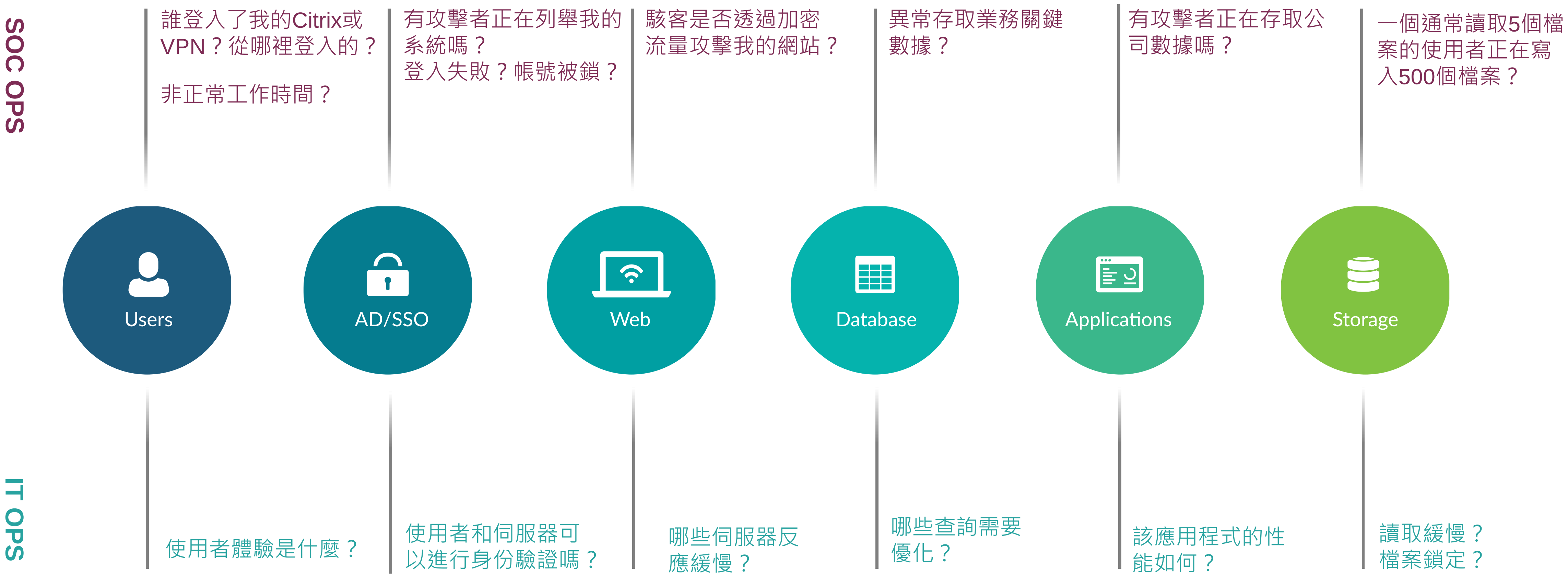
126 Techniques across 12 Tactics

92% coverage

6	Initial Access Techniques
9	Execution Techniques
14	Persistence Techniques
8	Privilege Escalation Techniques
16	Defense Evasion Techniques
10	Credential Access Techniques
17	Discovery Techniques
6	Lateral Movement Techniques
9	Collection Techniques
15	Command and Control Techniques
8	Exfiltration Techniques
8	Impact Techniques

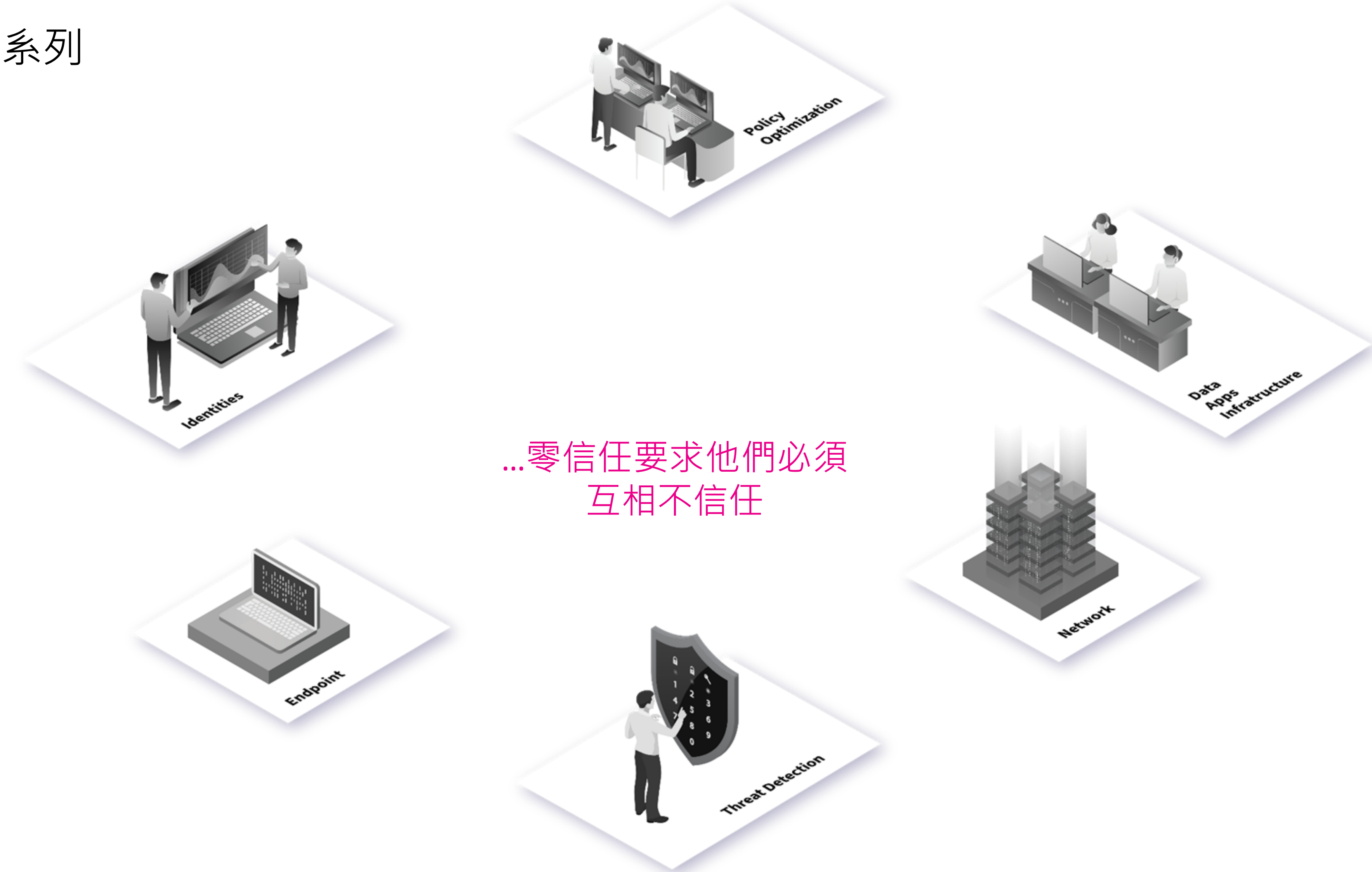
SOC AND IT OPS TEAMS 很難回答棘手的問題

In Real time and in Context



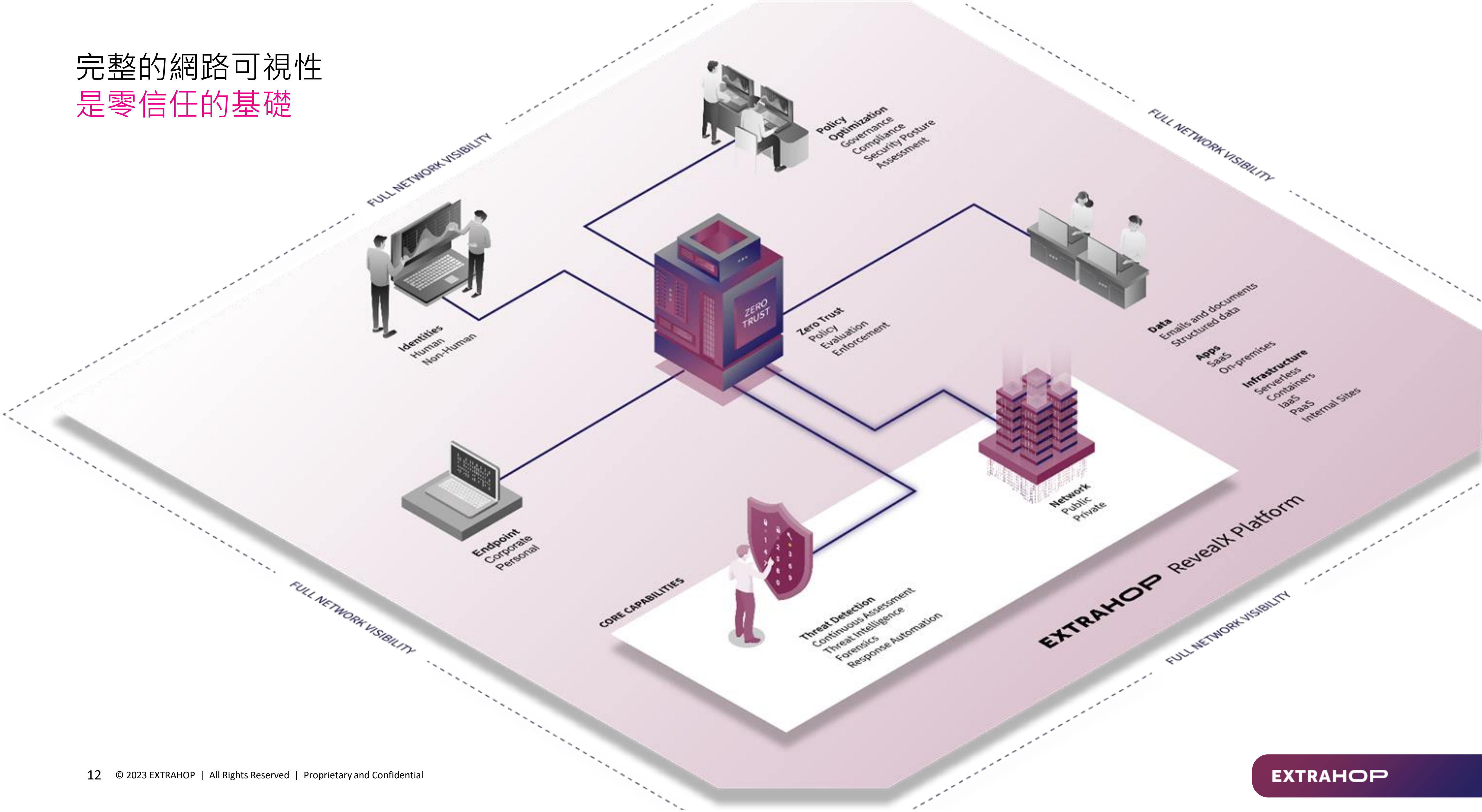
	Users	AD/SSO	Web	Database	Applications	Storage
SOC OPS	誰登入了我的Citrix或VPN？從哪裡登入的？ 非正常工作時間？	有攻擊者正在列舉我的系統嗎？ 登入失敗？帳號被鎖？	駭客是否透過加密流量攻擊我的網站？	異常存取業務關鍵數據？	有攻擊者正在存取公司數據嗎？	一個通常讀取5個檔案的使用者正在寫入500個檔案？
IT OPS	使用者體驗是什麼？	使用者和伺服器可以進行身份驗證嗎？	哪些伺服器反應緩慢？	哪些查詢需要優化？	該應用程式的性能如何？	讀取緩慢？ 檔案鎖定？

你的網路像一系列
孤立的島嶼...



...零信任要求他們必須
互相不信任

完整的網路可視性
是零信任的基礎



ExtraHop 支援 DoD(美國國防部) 的零信任能力

USER

- **1.4 特權存取管理**
- **1.6 行為識別,情境識別,生物特徵識別**

DEVICE

- **2.1 設備清單**
- **2.2 設備偵測與合規**
- **2.3 設備監控與即時檢查**
- **2.7 擴展偵測和回應** (XDR)

AUTOMATION & WORKLOAD

- **3.1 應用程式清單**
- **3.5 持續監控與持續授權**

DATA

- **4.4 數據監控與感知**
- **4.6 數據洩漏防護**

NETWORK & ENVIRONMENT

- **5.1 數據流對應**
- **5.2 軟體定義網路**

AUTOMATION & ORCHESTRATION

- **6.1 策略決策點和策略編排**
- **6.2 關鍵流程自動化**
- **6.3** 機械學習
- **6.5 安全編排自動化回應**
- **6.6** API 標準化
- **6.7** SOC 和事件回應

VISIBILITY & ANALYTICS

- **7.1 記錄所有流量**
- **7.2 安全資訊與事件管理 (SIEM)**
- **7.3 常見安全與風險分析**
- **7.4 使用者行為分析** (UEBA)
- **7.5 威脅情資整合**

零信任中 ExtraHop 的優勢

細緻的洞察

- 所有網路通訊
- 加密的東西向流量 企業級規模
- OSI第2至第7層封包檢查

為何對零信任那麼重要:

允許您識別並監控每一個裝置、使用者和網絡流量.

先進威脅偵測

- 五種形式的人工智能70項專利
- 自動回顧性檢測 ，自動關聯分析
- MITRE ATT&CK 覆蓋率

為何對零信任那麼重要:

使得持續監控和對任何偏離正常模式的快速響應成為可能.

自動化與編排

- 動態安全回應
- 與任何工具的整合
- 在安全生態系統中進行編排動作

為何對零信任那麼重要:

透過迅速的遏制和補救措施，最小化風險.

政策執行

- 持續監控並驗證網路通訊
- 即時流量處理

為何對零信任那麼重要:

提供即時智能，以便就安全政策和控制做出明智決策.

風險評估與管理

- 進階行為分析
- 即時威脅檢測

為何對零信任那麼重要:

賦予持續的、主動的風險識別、管理和評估能力，適用於網路上的每一個設備.

法規合規性

- 所有網路通訊
- 設備行為記錄
- 符合IS27001

為何對零信任那麼重要:

允許您識別並監控每一個裝置、使用者和網絡流量.

攤位編號：C118

EXTRAHOP

扭蛋 抽抽樂

1	Apple HomePod mini
2	Apple AirTag
3	質感環保購物袋
4	專屬打光師神器
5	旅行雙口充電頭
6	高級無線充電盤
7	伸縮三合一快速充電線
8	驚喜盲盒
0	來賓獎

參加辦法請洽現場工作人員

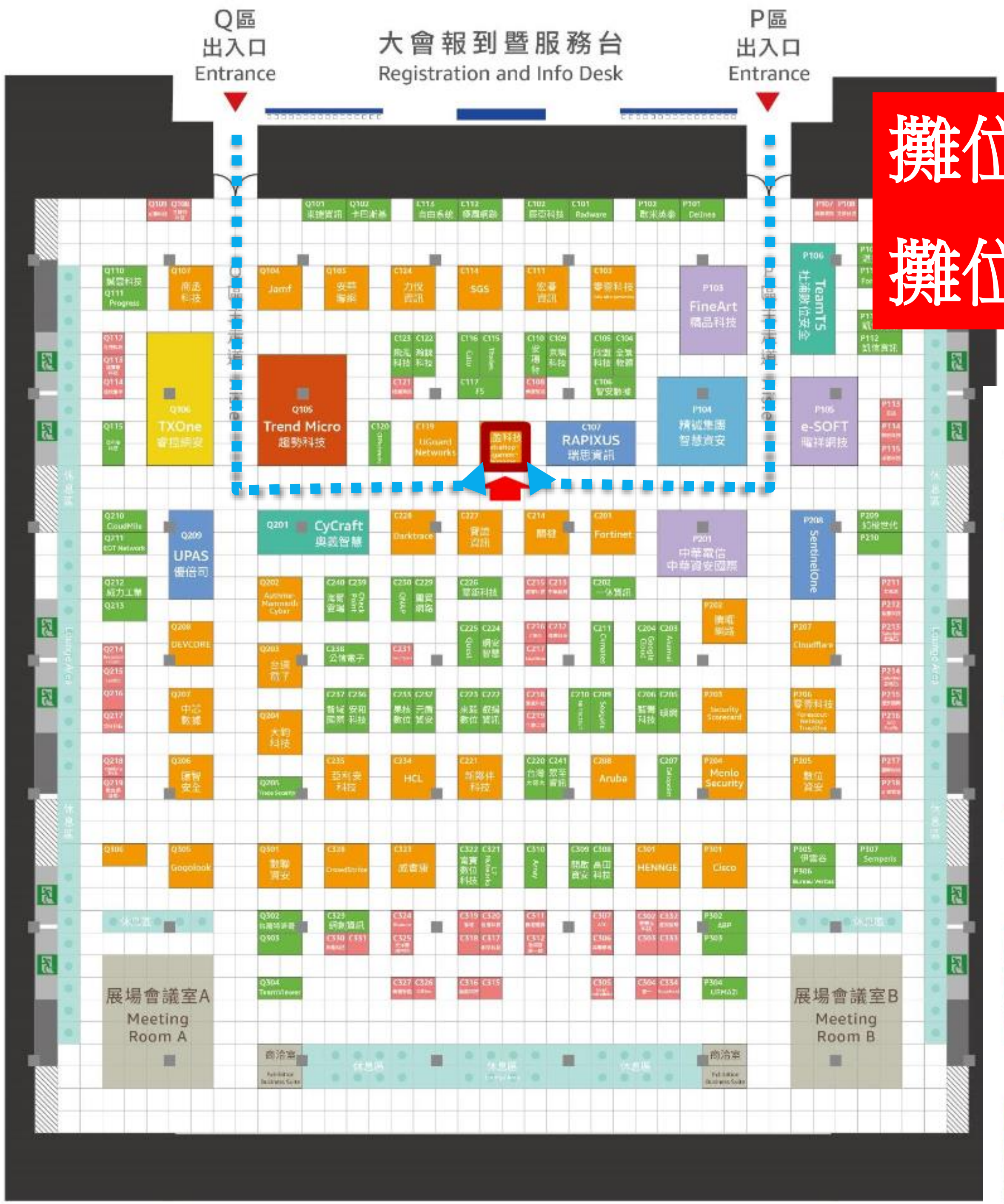
ExtraHop合作夥伴

NetFOS 逸盈科技

中芯數據 Core Cloud Tech

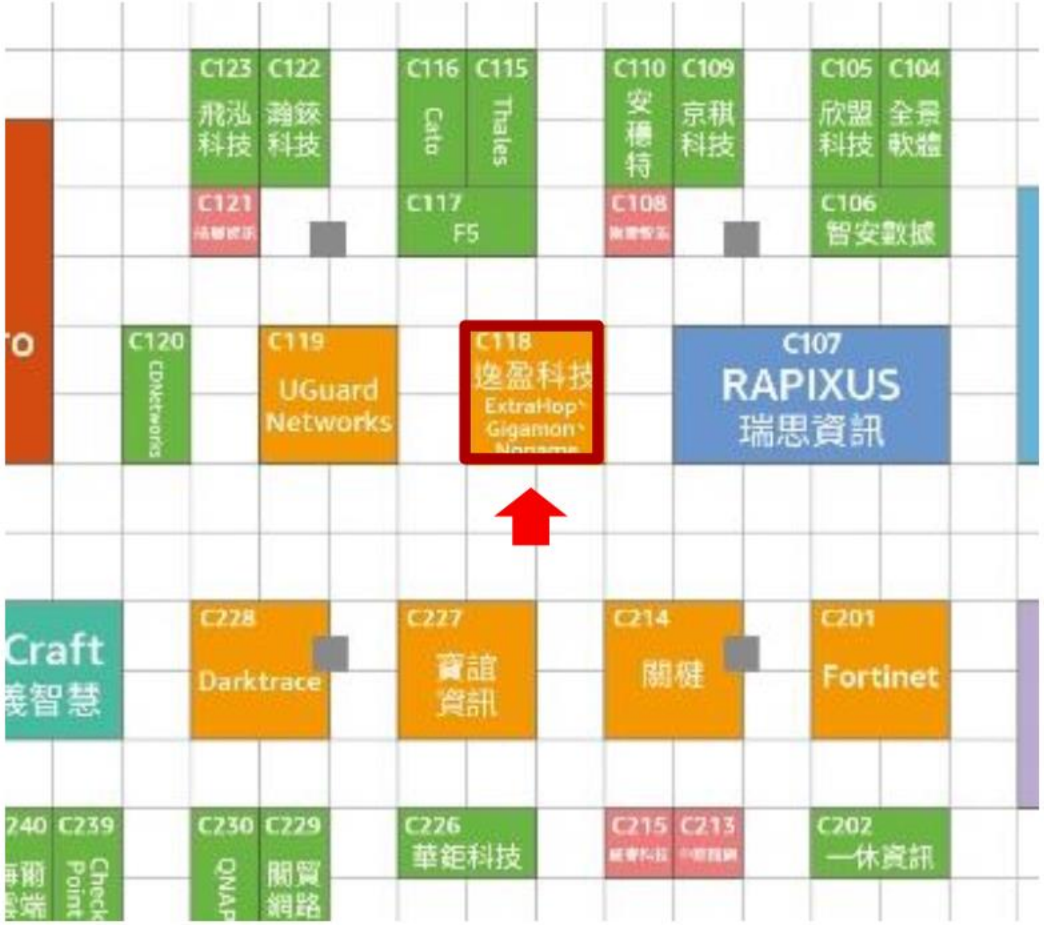
EXTRAHOP
EXTRAHOP
EXTRAHOP
RevealX NDR
更快速的揭示並回應網路威脅
EXTRAHOP
CYBER
RISK
REVEALED
EXTRAHOP
完整的網路可視性
EXTRAHOP
EXTRAHOP
EXTRAHOP

1F／展場平面圖



攤位名稱： ExtraHop 逸盈科技

攤位編號：C118



Thank You