



防護主動式攻擊：Sophos 人工智慧及 自動化解決方案

Frank Shen
Senior Sales Engineer

2023.11.22

SOPHOS

攻擊者大規模執行無數次攻擊

94%

的組織在過去
一年中至少經
歷過一次網路
攻擊

27%



Malicious
Email

27%



Phishing (including
spear phishing)

26%



Data Exfiltration
(by attacker)

24%



Cyber
Extortion

24%



Denial of Service
(DDoS)

24%



Business Email
Compromise

21%



Mobile
Malware

18%



Crypto
Miners

14%



Wipers

選擇過去一年中遭受的非勒索軟體網路攻擊組織所佔的百分比

各種進階攻擊已經司空見慣

23%

組織在去年遭受
主動攻擊者
攻擊

30%

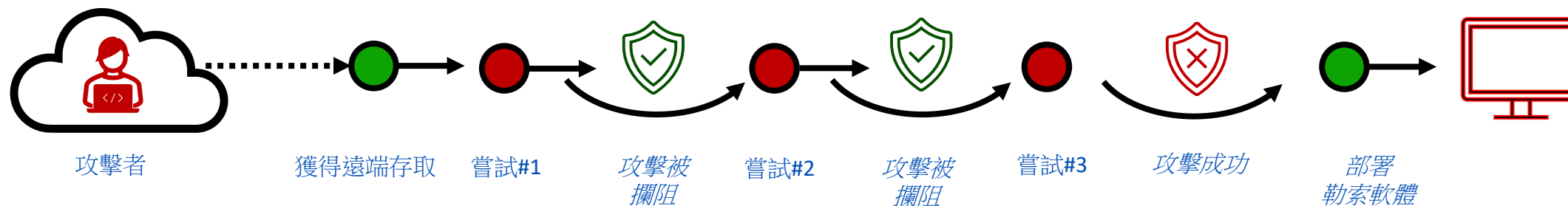
組織表示在2023
主動攻擊者是他們
擔心的網路攻擊

主動攻擊者發起的入侵，他們隨時手動操作鍵盤來動態調整其技術、策略和程序（TTP），以回應安全技術和防禦者的行動，並作為規避偵測的策略

主動攻擊者 vs 傳統攻擊手法



主動攻擊者特徵



- 主動攻擊者會使用多種技術、策略和程序，包括：
 - 利用安全漏洞滲透組織，然後橫向移動
 - 濫用防禦者使用的合法IT工具以避免觸發偵測
 - 即時修改攻擊以回應安全控制
 - 透過使用各種新技術，即時修改攻擊方式避免安全防護發現，直到找到入侵的方法

主動攻擊者的運作方式



多階段攻擊

攻擊結束地點與開始地點不同



利用現成的工具攻擊

以惡意方式使用混入攻擊的合法工具



未知漏洞

利用軟體中的弱點、缺陷或錯誤進行的攻擊



帳密外洩

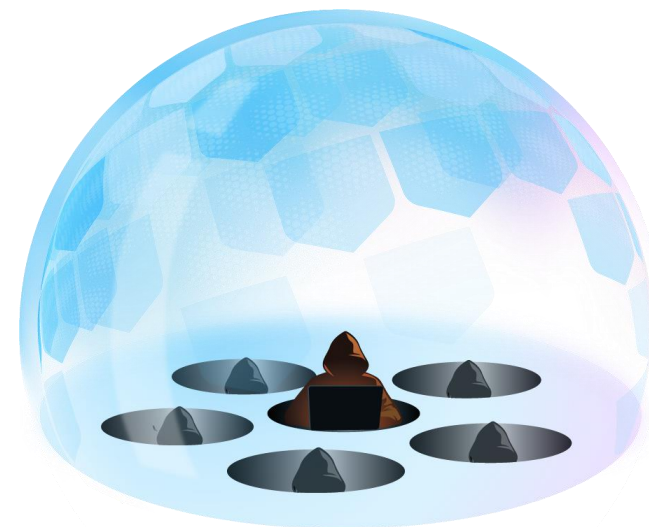
攻擊者登入而不是闖入開始的攻擊

如何阻止主動攻擊者?

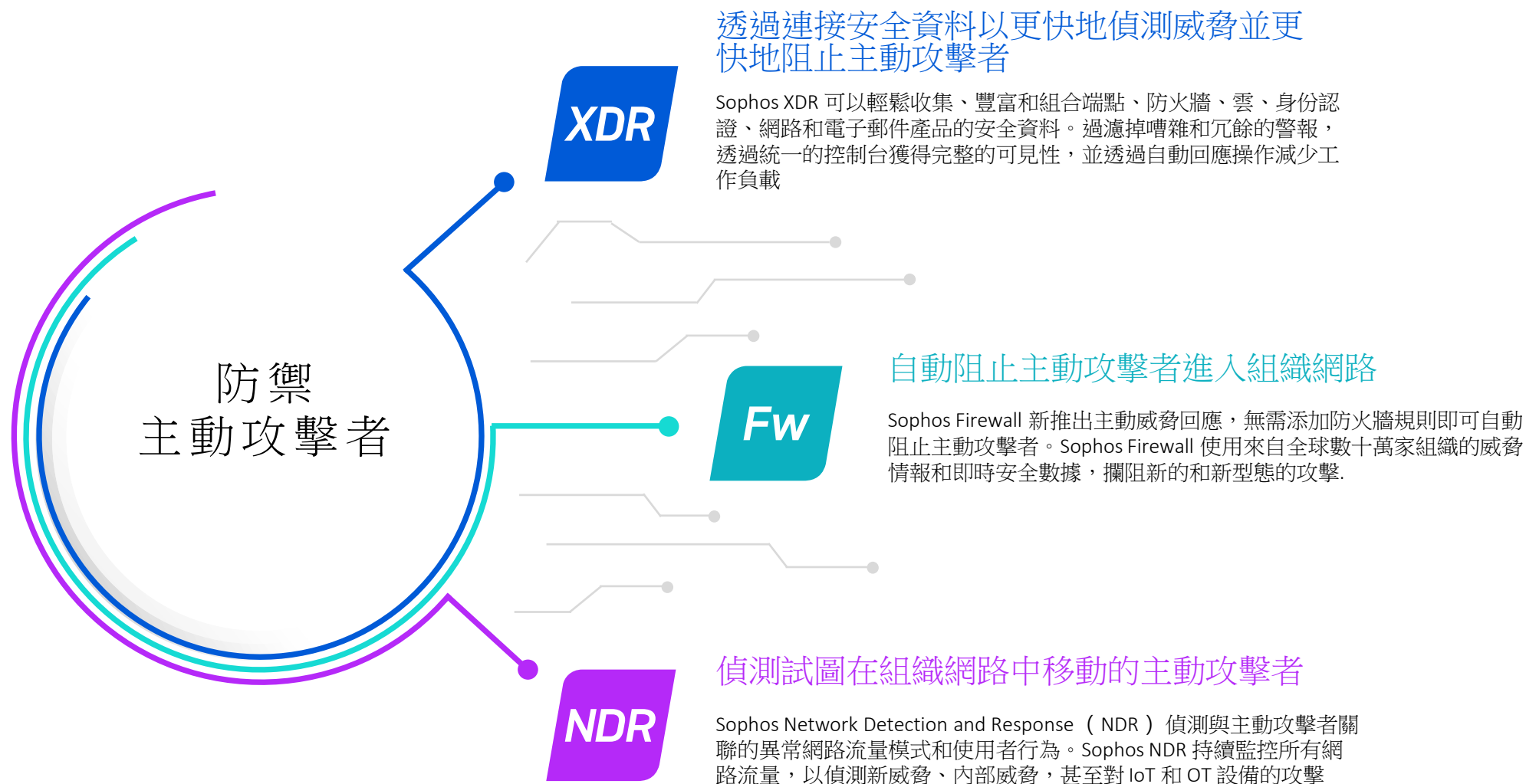


攻擊哪裡堵哪裡

VS.



主動攻擊者防禦



Sophos Firewall v20



防禦主動攻擊者

Sophos Firewall v20 全新功能

自動威脅回應

與 Sophos MDR 和 XDR 整合，阻止主動攻擊者



Active Threat Response (ATR)

自動攔阻與動態威脅源相關的流量，並封鎖網路上任何新的活動威脅



Dynamic Threat Feeds

防火牆用於自動攔阻與威脅相關的流量的新威脅情報源。第一階段威脅源將支援 Sophos MDR，未來將支援第三方威脅源



Synchronized Security IoC Telemetry

任何嘗試與被 ATR 攔阻的主機通訊的 Sophos 管理端點都將使用同步性安全查詢並深入了解

網路可擴展性和彈性

分散式企業的網路增強功能



IPv6

對IPv6支援的多項增強功能，包括 DHCPv6 和 BGPv6 路由，可提高 IPv6 互通性和 IPv6 Ready 認證



SD-WAN

新增支援多達 1024 個設定檔和 3072 個閘道，提高了 SD-WAN 部署的可擴充性



Site-to-Site VPN

VPN 多項增強功能，包括 IPsec 連線不中斷 HA 故障轉移、SNMP 狀態可見性和 SSL VPN 的 FQDN 支援

防護遠端工作者

啟動新的 SASE（安全存取服務邊緣）功能



ZTNA 閘道整合

Sophos ZTNA 閘道整合至 Sophos Firewall，可輕鬆安全地遠端存取本地應用程式



第三方 SD-WAN 整合

支援平穩、輕鬆地將流量接入到 CloudFlare、Akamai 或 Azure 的高性能全球骨幹網路。



Sophos DNS 防護

Sophos Firewall 完全支援具有合規性和安全性功能的新域名系統解析服務可供搶先體驗。

簡化管理

使複雜的網路比以往任何時候都更容易管理



物件使用尋找

快速確定網路物件在規則和政策中的使用位置



Azure AD 單一登錄

在 Captive Portal 上增加簡單的使用者身份驗證，同時在群組政策增加新的組匯入選項



網路介面啟用/停用

快速輕鬆地停用或啟用防火牆上的介面，設定部會因此消失

And more!

Active Threat Response

擴展同步性安全

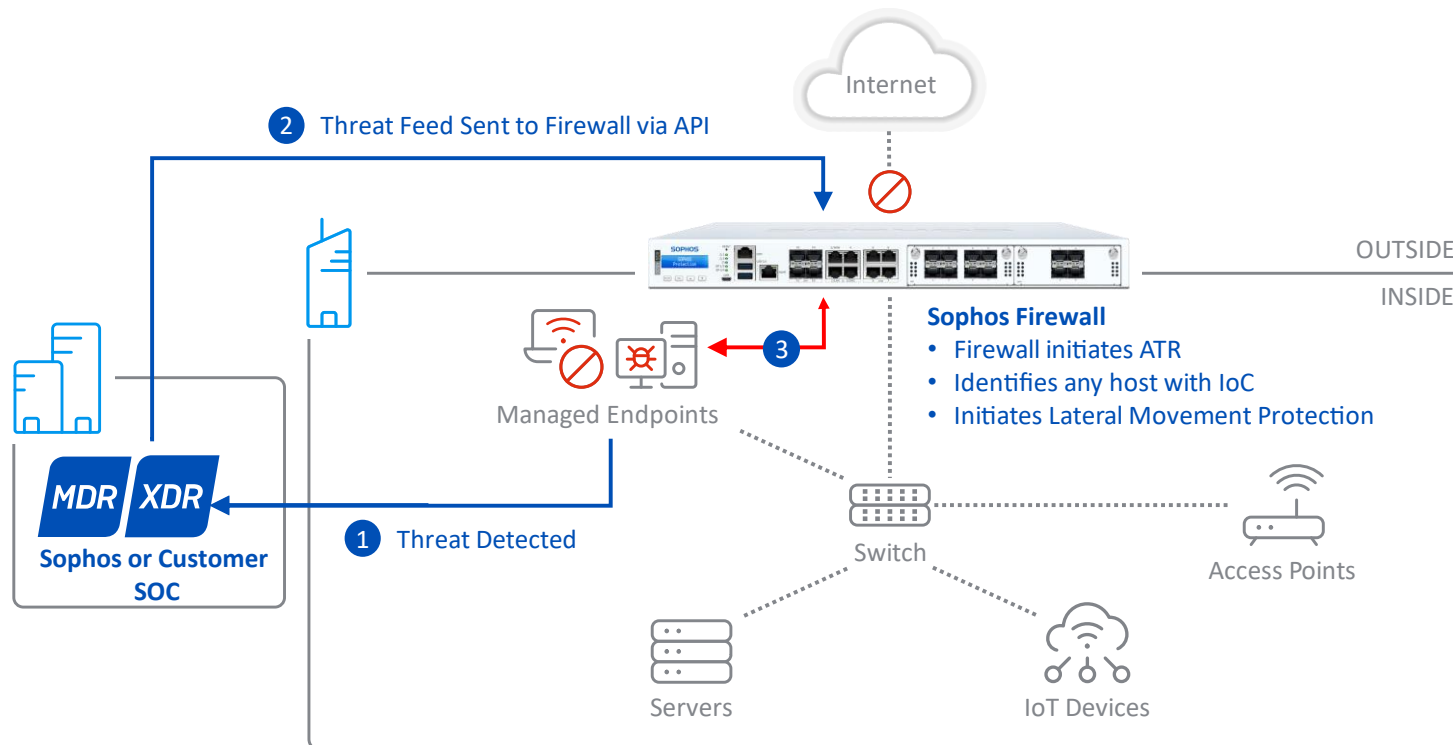
可擴展的同步安全性...

- Sophos MDR / XDR 威脅獵捕
- 使用動態威脅源
- 使用第三方威脅源(未來)

相同的自動回應

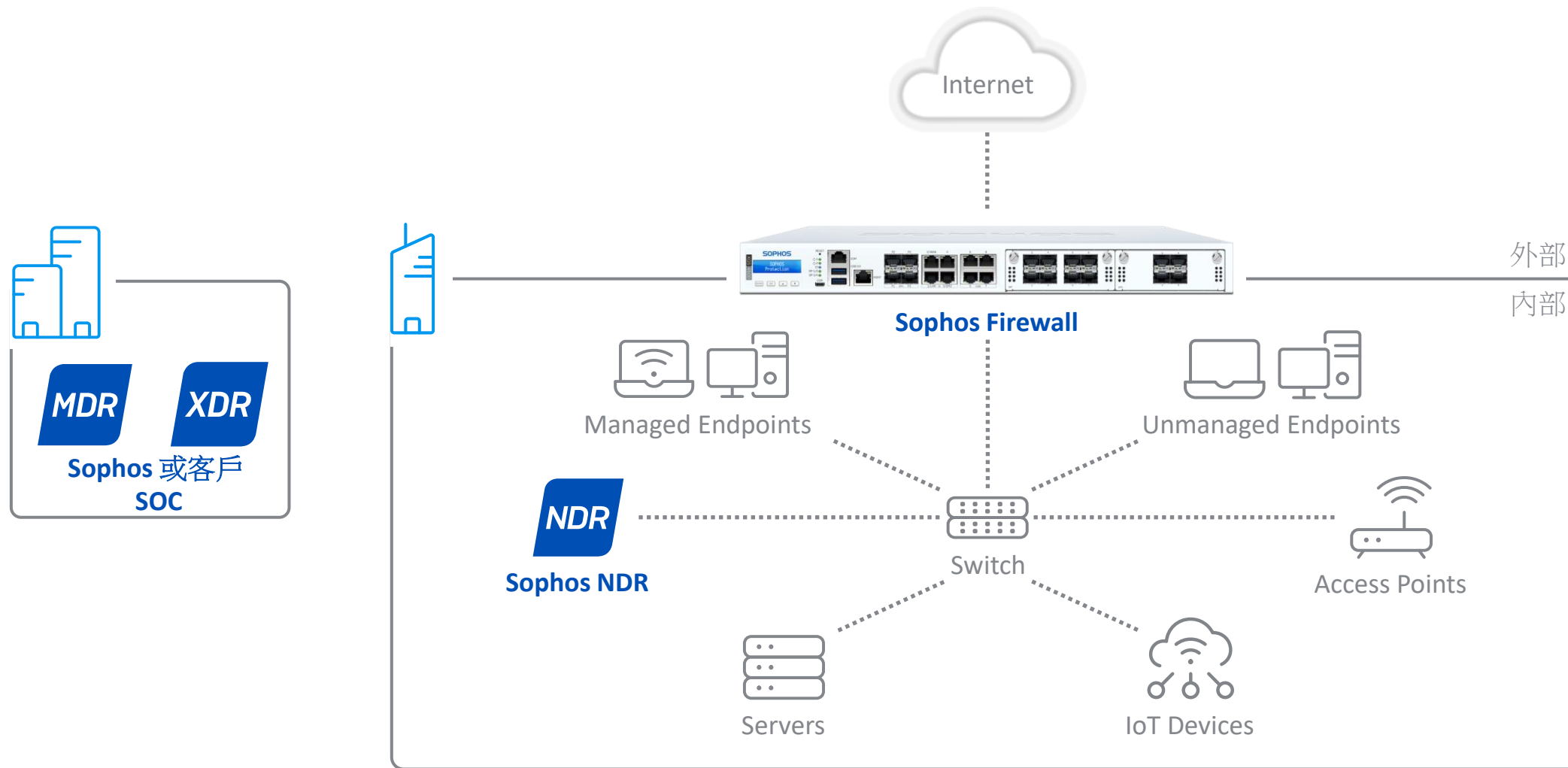
- 自動阻止威脅從網路內散播出去
- 自動與防護端點聯防，以阻止來自受感染主機的流量
- 自動防止橫向擴散
- ZTNA 阻止與應用程式直接連線
- 一旦威脅被根除，自動恢復所有連線

即時回應 - 無需管理員操作或設定防火牆規則

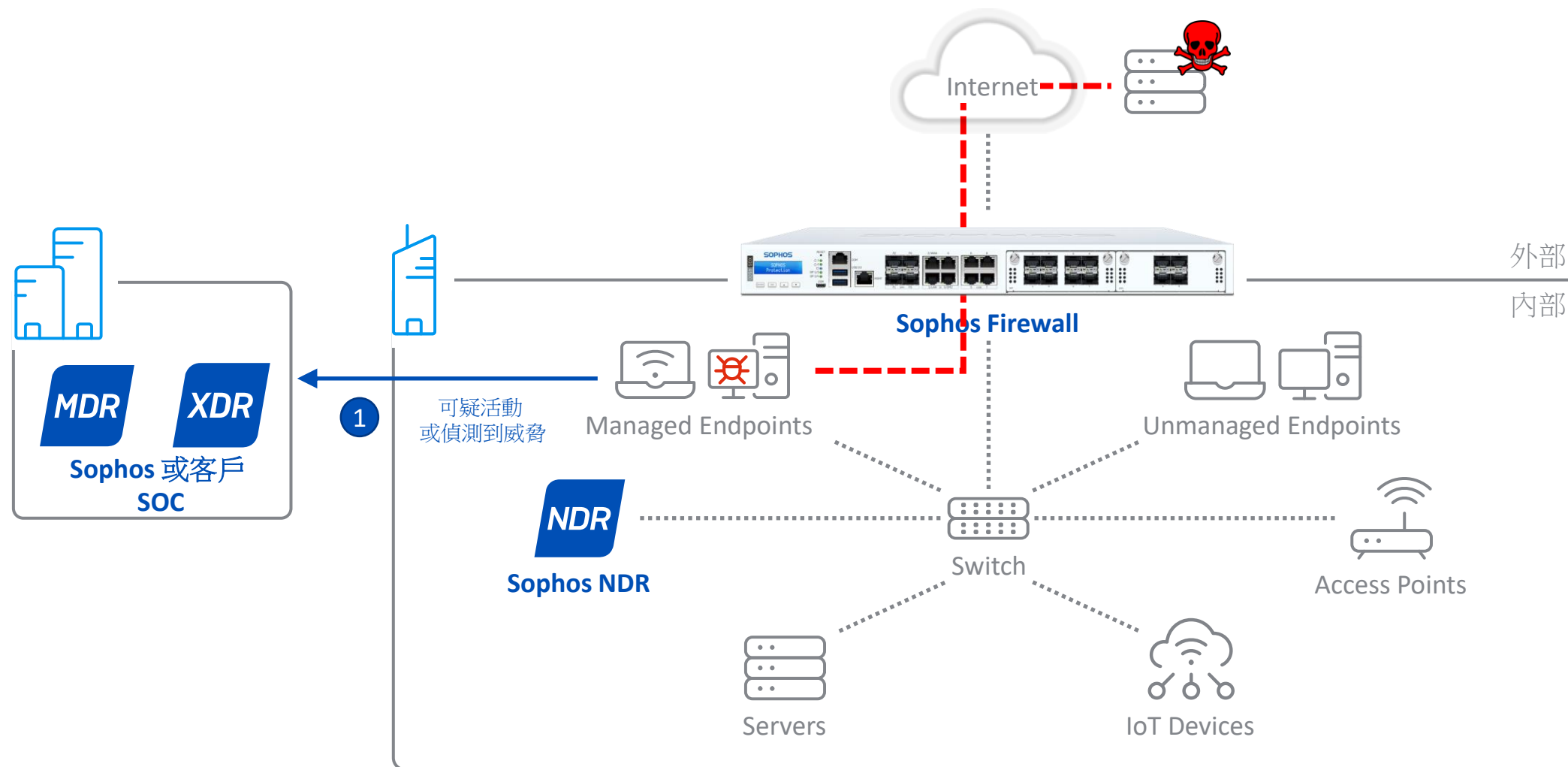


同步性安全

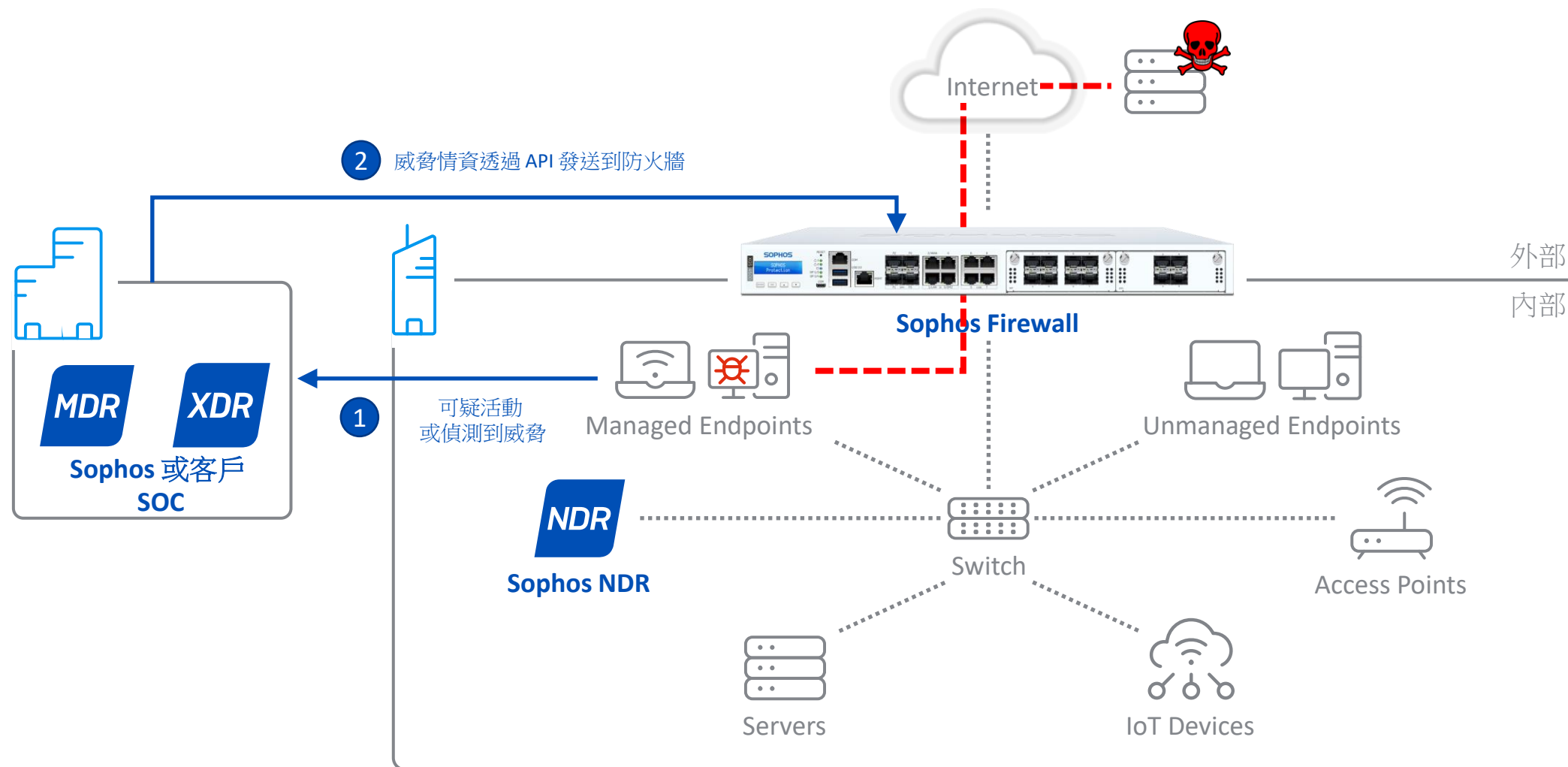
Active Threat Response 運作方式



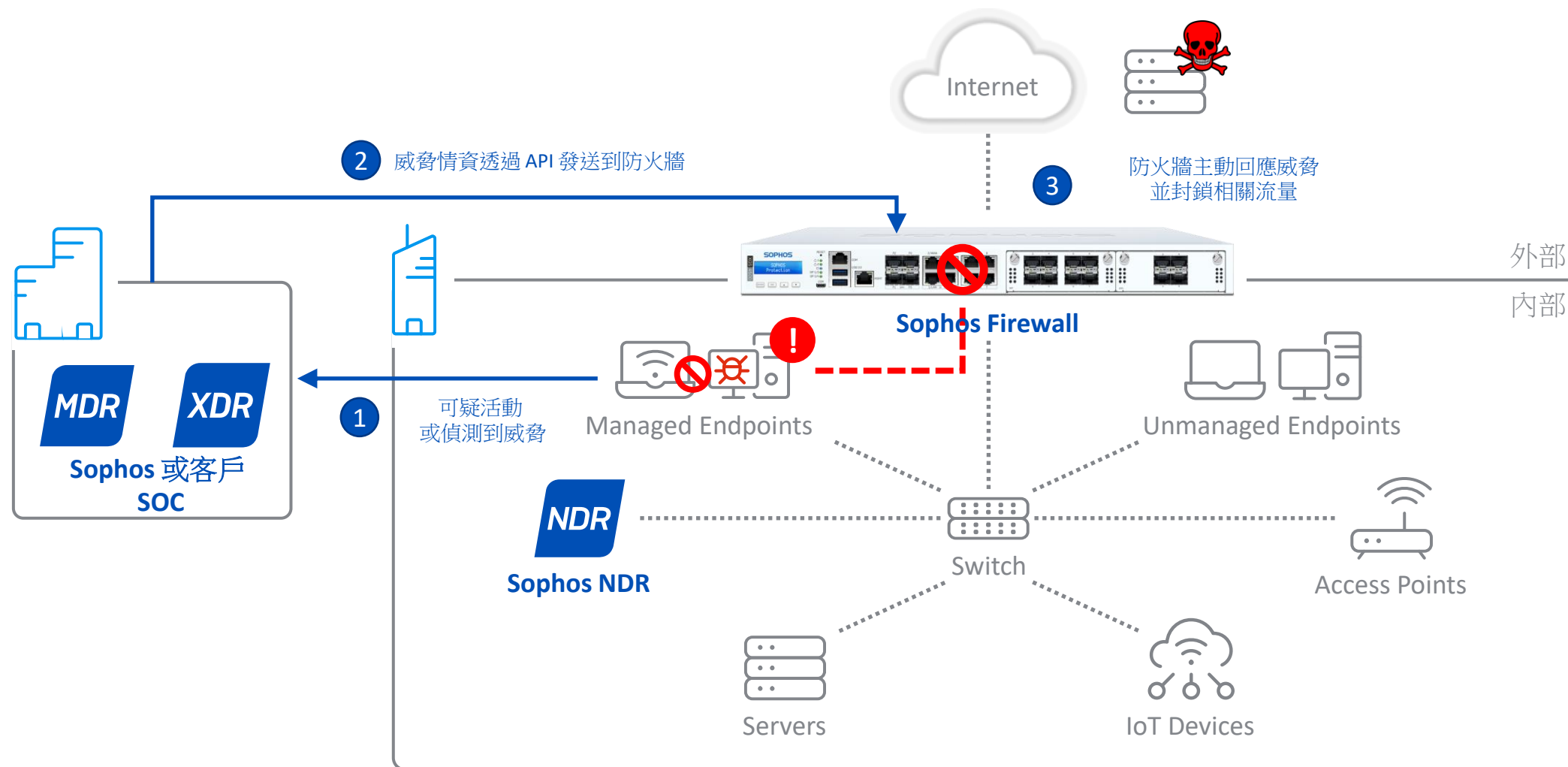
Active Threat Response 運作方式



Active Threat Response運作方式

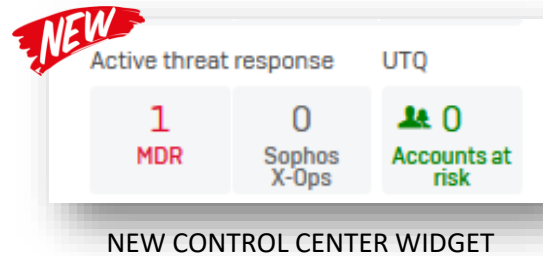


Active Threat Response運作方式



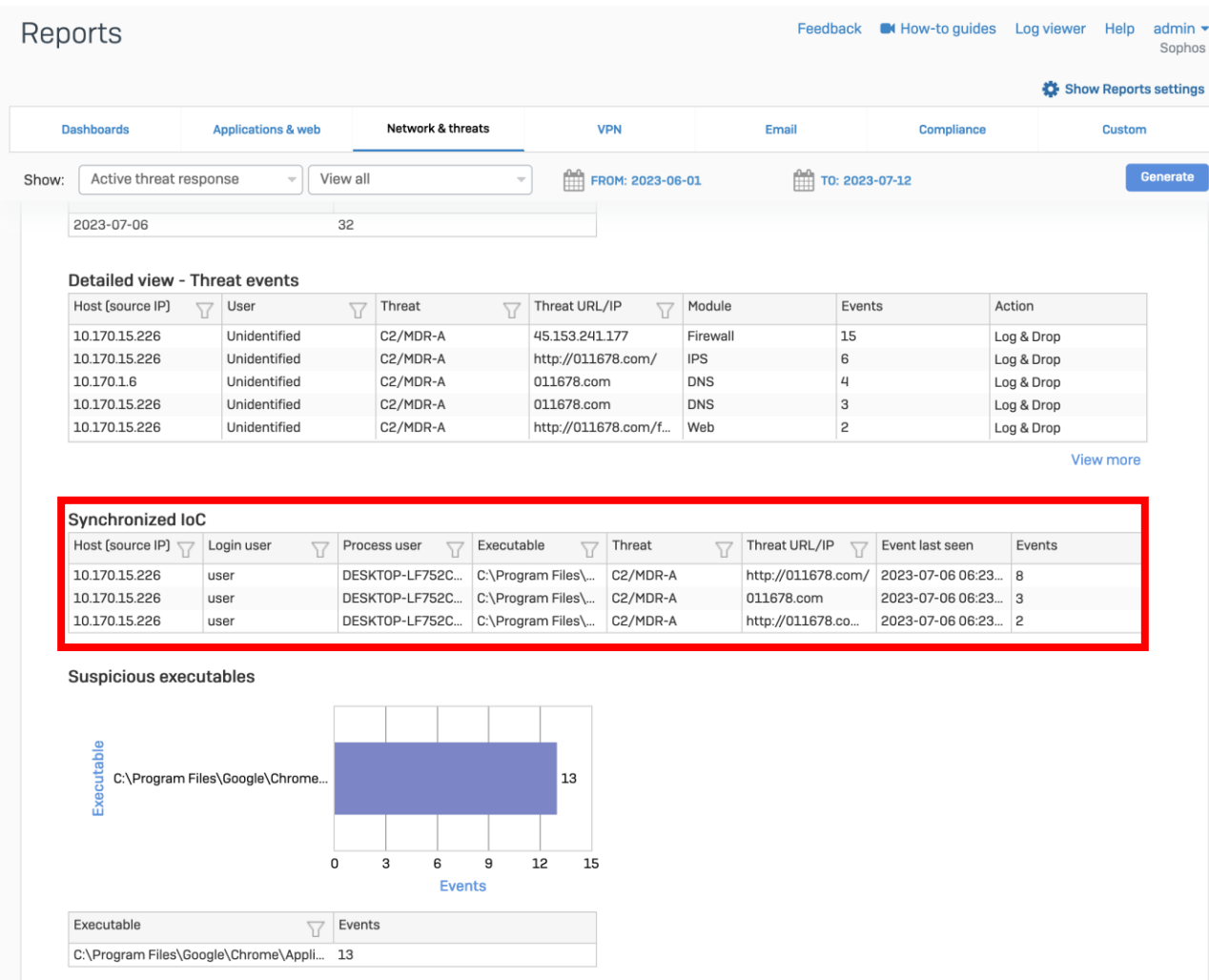
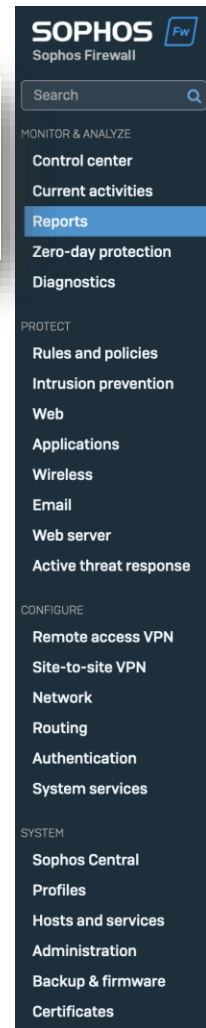
即時回應 - 無需管理員操作或設定防火牆規則

Active Threat Response IoC 遙測



即時洞察

- “控制中心”小工具可標記網絡上的任何活動威脅
- 任何嘗試與被封鎖的威脅源連線的受管理端點都會觸發 IoC 遙測資料收集
- 主機、使用者、程序、可執行檔、威脅資訊、時間、事件數量



可擴展的威脅源

MDR 威脅情資

- 透過 API 推送威脅情資
- Sophos MDR
- 第三方MDR供應商

第三方情資

- 拉取威脅源
- 外部發送
- 稍後推出

X-Ops 威脅情資

- 舊名為進階威脅防護(ATP)
- 特徵碼方式更新威脅情資
- 既有ATP情資
- 惡意 domains, URLs, IPs

The screenshot displays the Sophos Firewall management interface. On the left is a dark sidebar with a search bar and a menu organized into three sections: MONITOR & ANALYZE (Control center, Current activities, Zero-day protection, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server), and CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services). The 'Active threat response' option is highlighted in the PROTECT section. The main content area is titled 'Active threat response' and includes links for 'Feedback', 'How-to guides', 'Log viewer', and 'Help'. It features three tabs: 'MDR threat feeds' (marked with a red 'NEW' badge), 'Third-party threat feeds' (marked with an orange 'FUTURE' badge), and 'Sophos X-Ops threat feeds' (marked with a green checkmark). Below the tabs are links for 'Add global network and threat exceptions' and 'Logs'. The 'Xstream MDR response' section contains a toggle for 'Enable Xstream MDR response' (set to ON), an 'Action' dropdown (set to 'Log only'), and a 'Logging' status (set to 'Enabled' with a 'Change log settings' link). An 'Apply' button is located at the bottom of this section.

Sophos Firewall 內建 ZTNA Gateway

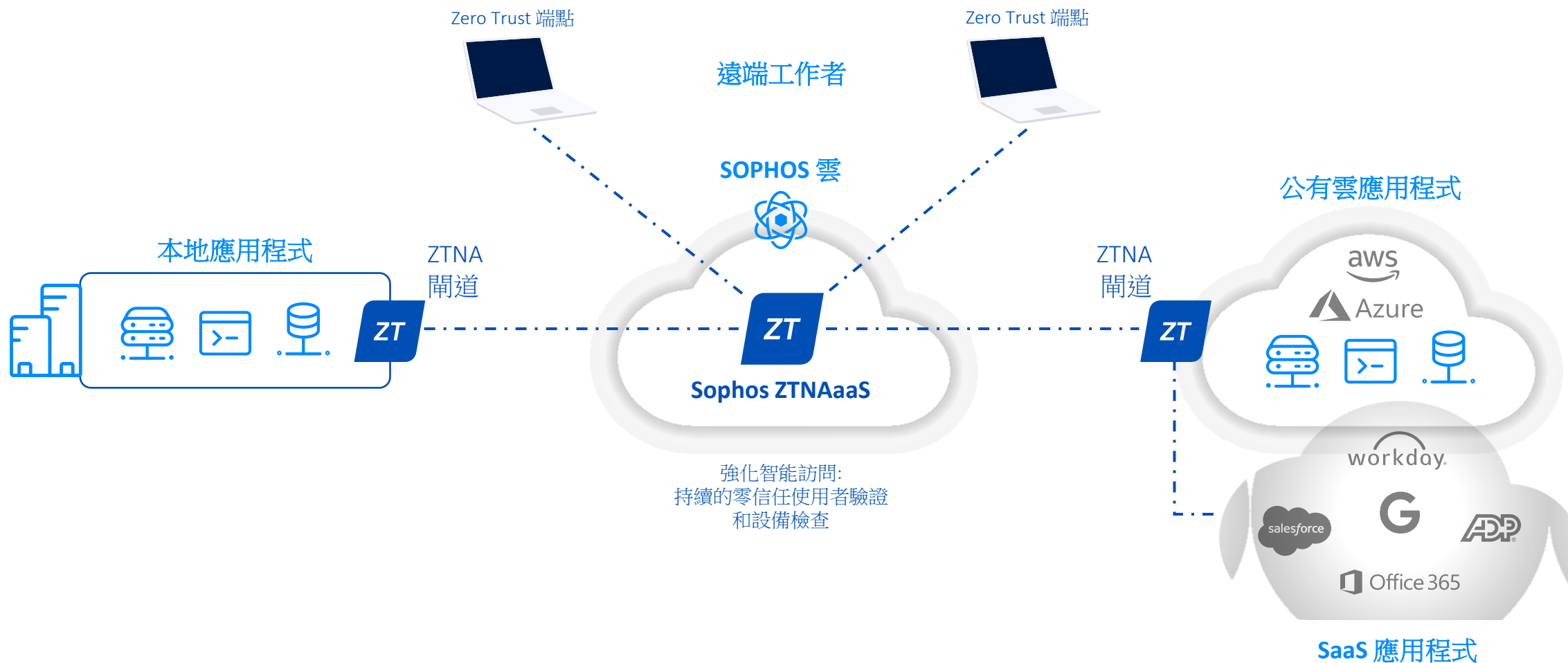
所有 Sophos 防火牆現在都內建 ZTNA 閘道
零信任的使用比以往任何時候都更容易



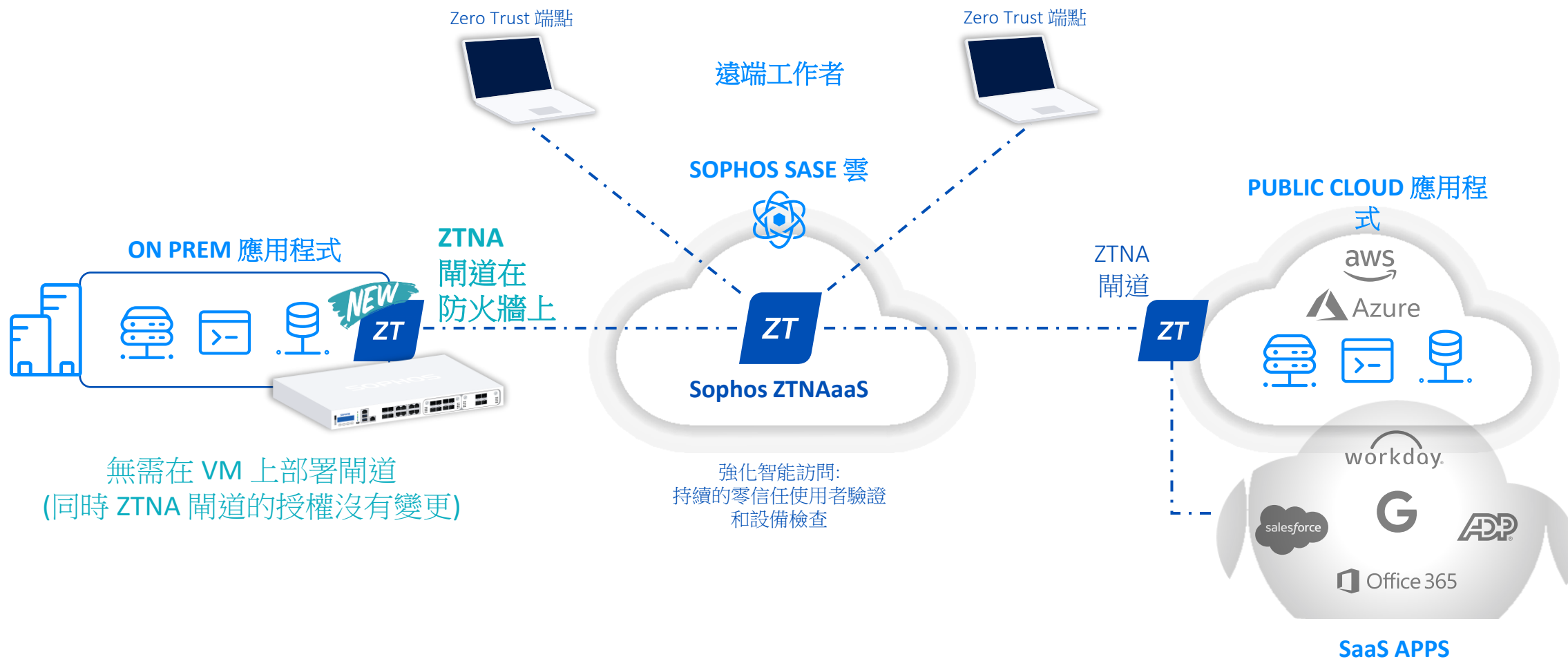
- 整合零信任連接器
- 零接觸部署
- 無需其他硬體設備
- 從現在開始，每個防火牆都是一個 ZTNA 閘道
- 支援各種平台
 - XGS 系列
 - 雲
 - 虛擬/軟體設備
- 透過Sophos Central 單一控制台管理

零接觸 - 零信任

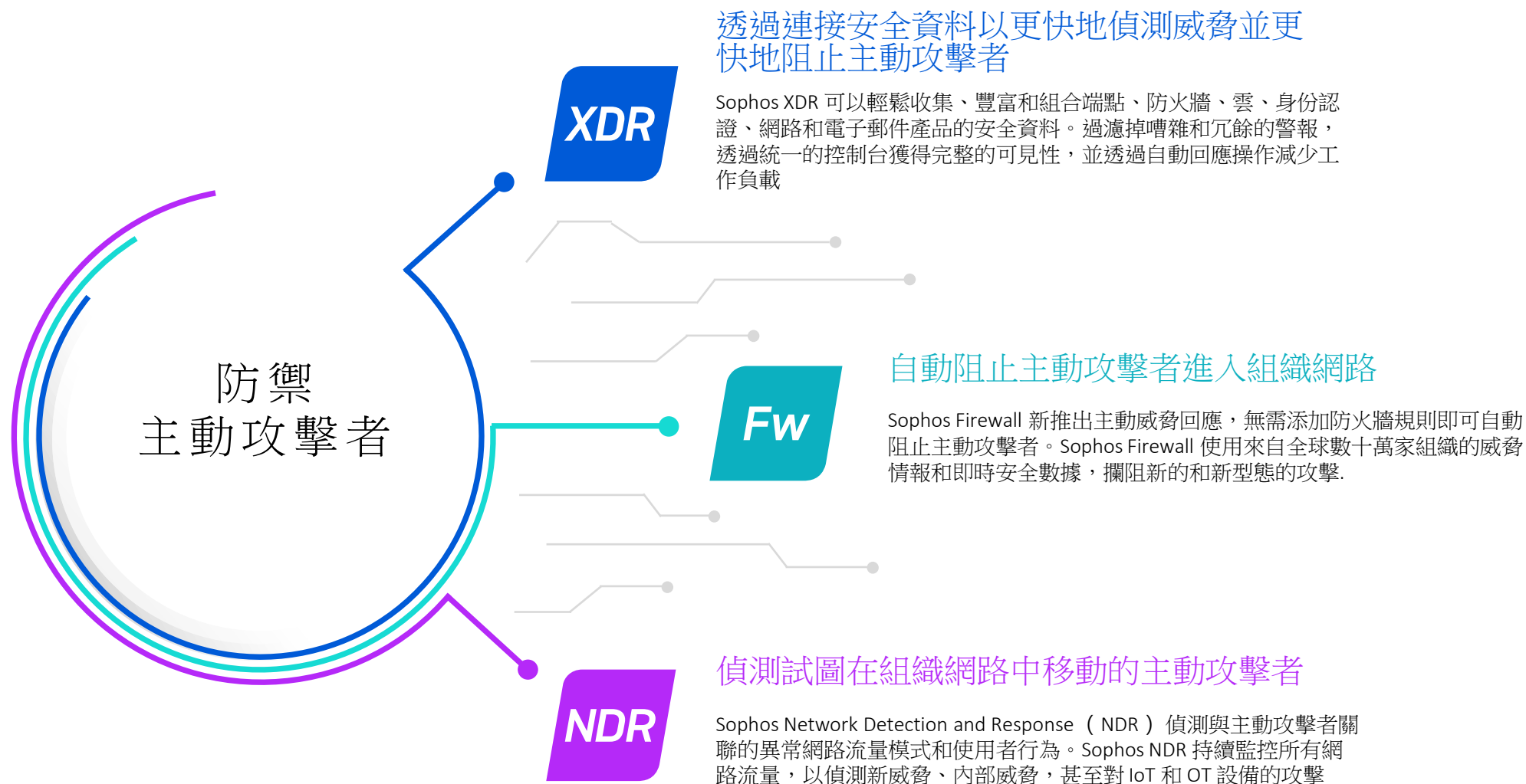
ZTNA as a Service – 運作原理



ZTNA閘道整合至防火牆- 零接觸零信任



XDR

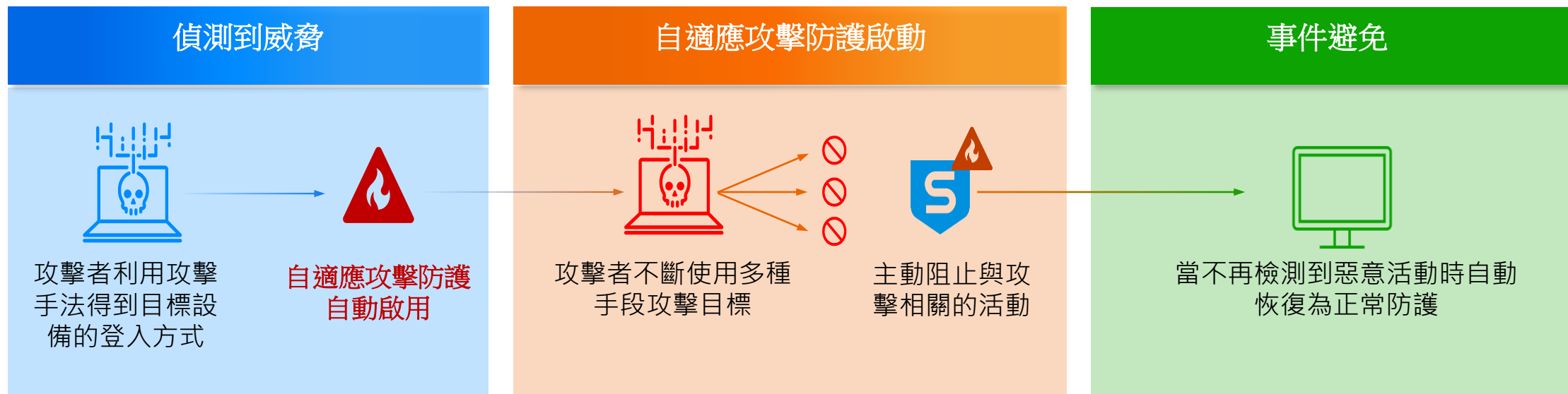


阻斷主動攻擊

	行為模式防護	自適應 攻擊防護	嚴重 攻擊警告
範圍	個別設備	個別設備	廣泛設備
優點	透過行為模式引擎攔阻主動攻擊者的早期階段	提高保護靈敏度以防止損壞	提醒客戶需要立即回應攻擊事件
觸發	行為模式規則	偵測到駭客工具集	高影響的主動攻擊者指標，包括駭客組織的相關性和門檻值
警報	“啟動防護罩!”	“啟動防護罩!”	“緊急事件!”

自適應攻擊防護

動態適應人為主導攻擊的防禦



- 如果不受阻礙，手動攻擊者更有可能入侵目標
- 自適應攻擊防護動態使用產生過度激進的保護，會擾亂日常維運

自適應攻擊防護範例

PaperCut 列印管理軟體中的一個漏洞導致勒索軟體攻擊

```
"spid": "[2124:133210265358704510]",  
"win32Path": "<d>\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",  
"newSpid": "[6580:133268400518887019]",  
"cmdline": "powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAaGIAagBLAGMAdAAgAEI  
"pwin32Path": "<d>\\Program Files\\PaperCut NG\\runtime\\win64\\jre\\bin\\pc-app.exe"
```

PaperCut

cobaltstrike

21:18

ΔΓΞΓΔ

21:19

AnyDesk
TightVNC

04:20



ADVANCED PORT SCANNER



LOCKBIT

08:58



Enables Adaptive Attack Protection

Exec_27a (T1059.001)

阻止CobaltStrike 工具呼叫執行
PowerShell shellcode

Disrupt_6a (T1219)

阻止遠端管理工具在自適應攻擊
防護模式下執行

潛在有害程式

特徵碼比對埠掃描程式
是否為PUA

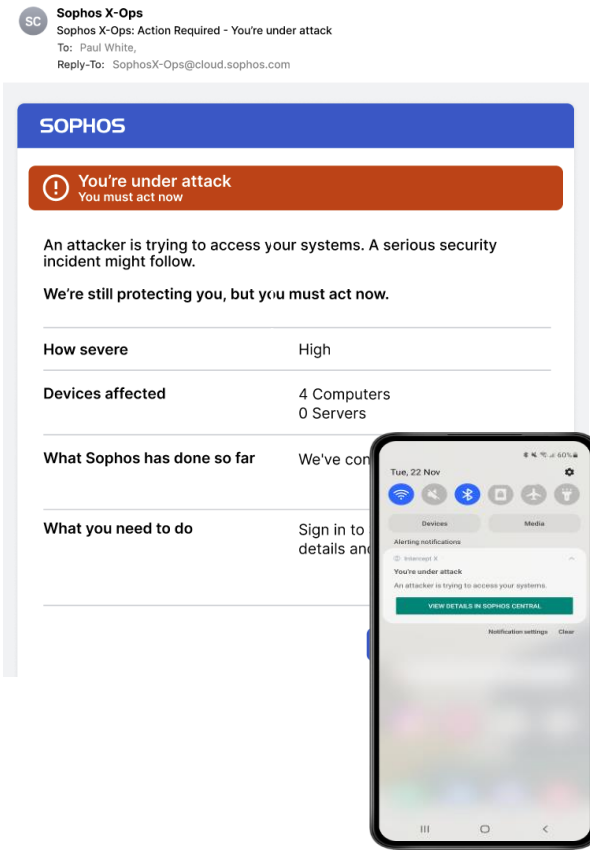
Disrupt_2a

在自適應攻擊防護模式下阻止執
行不受信任的EXE或 DLL
(勒索軟體 payload)

嚴重攻擊警告

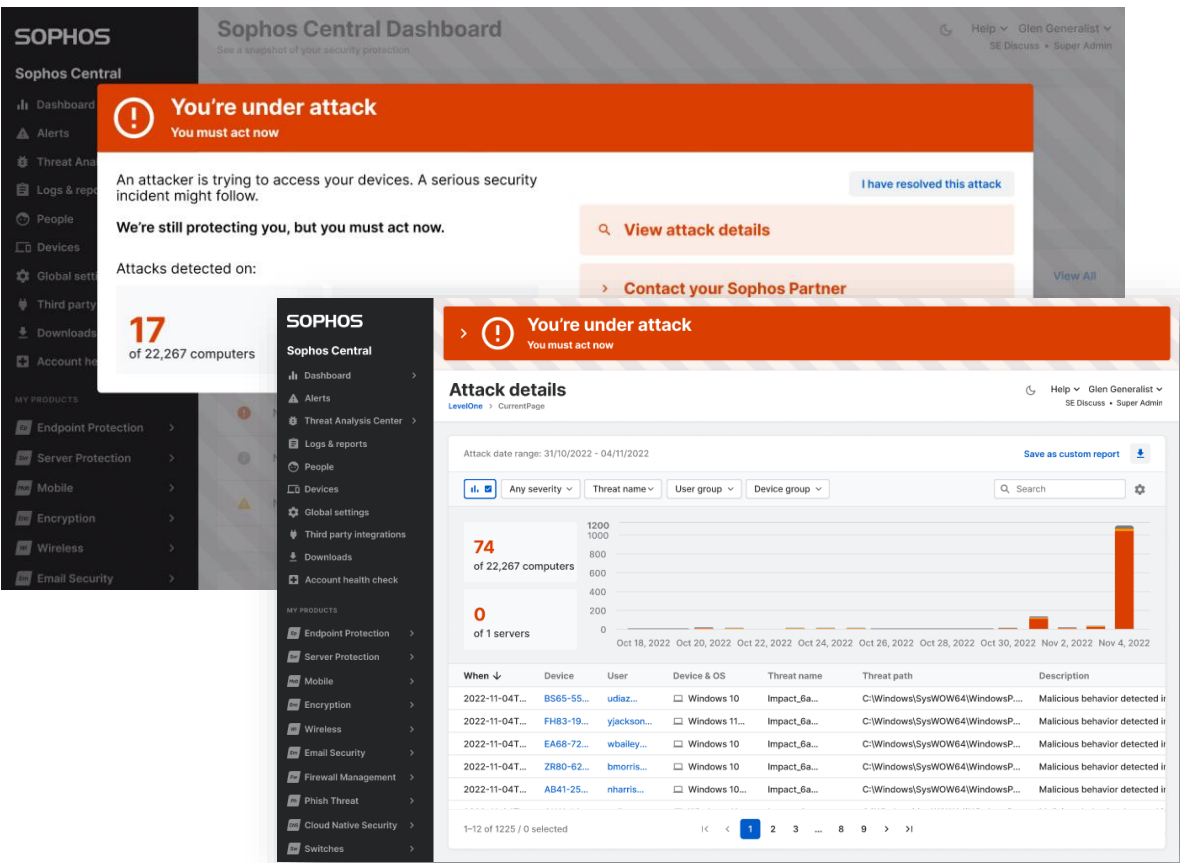
通知

透過電子郵件和手機
快速通知客戶



資訊

提供攻擊脈絡和詳細資訊



解決

尋求合作夥伴、事件回應
或自我修復





第三方整合

連接安全數據以更快地偵測威脅
並更快地阻止主動攻擊者

- 與第三方端點、防火牆、網路、雲、電子郵件、生產力和身份認證產品整合
- 使用既存端點。無需卸載和更換
- 與 Sophos MDR 產品一致



最佳化 分析師感受

在所有關鍵受威脅處進行有效率
偵測、調查和回應可疑活動

- 全新偵測使用者介面 - 一目了然地查看最重要的資料，以便快速調查
- 案例管理 - 通過新的協作工具和回應動作提高效率
- 簡化（無 SQL）搜索，達到快速搜尋

XDR Sophos XDR 產品擴展

整合第三方解決方案



整合 Sophos、Microsoft、端點和生產力均免費提供。
其他集成包和 Sophos NDR 是收費的附加元件

從現有技術投資中獲得更多投資回報

將現有工具整合到 Sophos XDR 平臺中。無需拆卸和更換

廣泛的第三方整合生態系統

端點、防火牆、網路、電子郵件、身份認證、雲和生產力解決方案

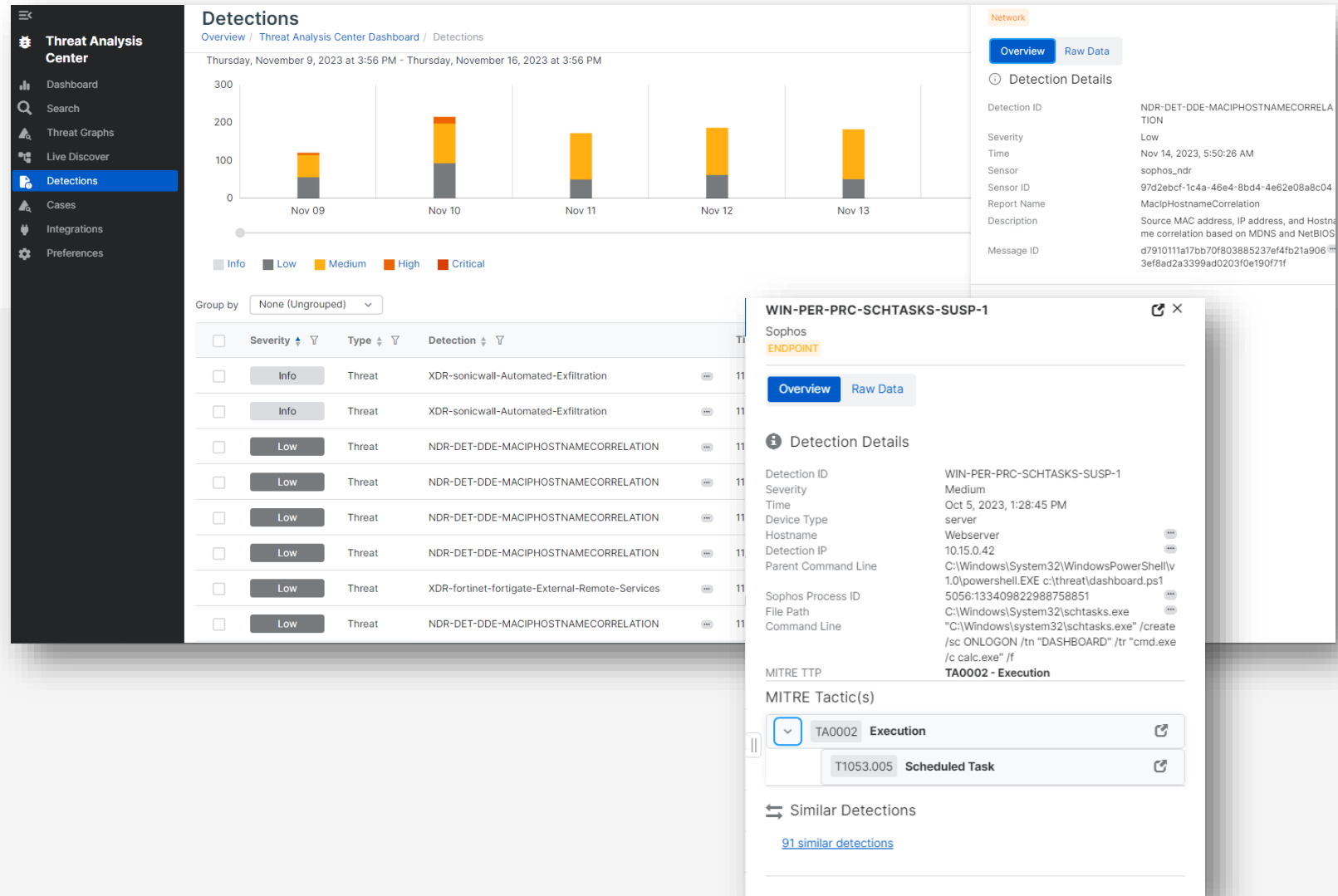
從單一控制台實現完全可見性

查看所有關鍵攻擊面中的威脅。
對警報進行分析、關聯和優先排序，以加快調查速度

更適合分析師: 全新使用者介面

更多關注 更好的脈絡

- 提供每個偵測最重要數據的清晰視圖，包括來自**第三方**來的數據
- 擴充透視和快速連結到預設的「Live Discover」查詢，以**提高調查效率**
- 方便的「Live Response」存取：透過安全終端連接到設備進行調查和修復問題



更適合分析師: 案件管理和事件回應

提高分析師的效率和協作能力

- 案件 '**Notebook**'. 在整個調查過程中收集證據並組織調查工作
- **MITRE ATT&CK 對應**. 識別防禦漏洞並確定改進的優先順序
- **回應動作**. 只需按一個按鈕即可執行動作以遏制潛在威脅
- **MDR客戶**: 與 Sophos 專家協作，作為自己團隊的延伸或當作自己的團隊

The image displays two overlapping screenshots of the Sophos XDR (Extended Detection and Response) interface. The top screenshot shows the 'Case Notebook' for a new case #106522, which is in a 'Critical' and 'In Progress' state. The notebook interface includes a sidebar with navigation options like Dashboard, Search, Detections, Cases, Preferences, Configurations, and Integrations. The main area of the notebook is titled 'Welcome to your Case Notebook!' and provides instructions on how to document and organize work. It features a toolbar with buttons for 'Add Block' and 'Show: All Blocks', and a search bar. Below the instructions, there are four blocks: 'Plain Text' (Rich text formatting), 'Table' (Create custom tables), 'Attachment' (Images, Files, etc.), and 'Data Lake Search' (Advanced searching).

The bottom screenshot shows the 'Detection Details' for a specific detection. The detection is named '[Detection Name] Firewall' and is associated with the IP address 10.55.109.173. It was detected on Feb 18, 2022, at 7:21:15 PM. The detection details include a list of related processes and network connections. On the right side, there is a 'Source Specific Details' section with a table showing various attributes like Message, Classification, Decision, Direction, and Priority. Below this, there is a 'MITRE Tactic(s)' section with a table showing the mapping of detection events to MITRE tactics. The bottom screenshot also includes a 'Case Summary' section with a summary of the detection and a list of related events.

更適合分析師: 簡化（無 SQL）搜索

快速調查和獵捕威脅

- 極大化地提高不同層級的安全分析師和IT管理員的效率
- 透過搜索 IOC 和其他資料（如 IP 地址或使用者名稱）在 Sophos 數據湖中尋找特定數據
- 直觀的搜索構建器、自由文本和提示 Lucene 選項使客戶能夠更快地找到所需的數據，而無需 SQL 專業知識！
- 可設定的結果檢視，有助於組織數據

The screenshot displays the Sophos Threat Analysis Center Search interface. The top navigation bar includes 'SOPHOS Beta', 'Dashboards', 'My Products', 'Threat Analysis Center', 'Alerts', 'Reports', 'People', and 'More'. The left sidebar shows the 'Threat Analysis Center' menu with options like 'Dashboard', 'Search', 'Threat Graphs', 'Live Discover', 'Detections', 'Investigations', 'Integrations', and 'Preferences'. The main search area has a 'Search' tab selected. A search bar contains 'Endpoint Data' and a '+ Search or select' button. A 'Last 7 days' filter is set, and a 'Search' button is visible. A 'Commonly used' dropdown menu is open, showing fields for Endpoint (Device IP, Hostname, Username), Process (Process Name, Parent Process Name, Process ID, Parent Process ID, Command Line), HTTP (Source IP, Destination IP), and Network (Destination IP, Destination Port). Below the dropdown, a table displays search results with columns for Time, Process, HTTP, and Network.

Time	Process	HTTP	Network
October 4 2023	running_processes_windows_sophos	Win11-4	Sophos
October 4 2023	running_processes_windows_sophos	Win11-4	Sophos
October 4 2023, 01:59:07	running_processes_windows_sophos	Win11-4	Sophos
October 4 2023, 01:59:07	running_processes_windows_sophos	Win11-4	Sophos
October 4 2023, 01:59:07	running_processes_windows_sophos	Win11-4	Sophos

XDR - Demo

展示場景

- 完整影片

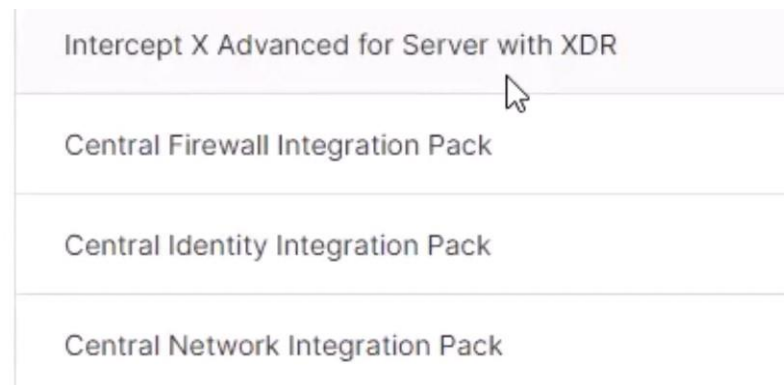
<https://vimeo.com/884159696/4f60e69e35>

- 展示與第三方解決方案 – Okta 整合
- 透過 XDR 偵測到異常行為
- 藉由 Okta 將有問題的帳號停用

準備動作

- XDR License
- 第三方設備整合包(Integration Pack)

- 設定 Okta 整合
- 設定 Data Injection 可以傳送資料給 Okta



Add Okta API Token Credential ×

1 Details 2 Credential

Credential Name *
Okta token credential

Description

Permissions *
Select your credential's access permissions here. This doesn't enable or disable them.
Set users' temporary password ⓘ ...

Integrations with Access *
Select the integrations that can use this credential.
Response Action ⓘ Data ingestion ⓘ



Expiration Date

Response Action will have access to:
Suspend users Unsuspend users

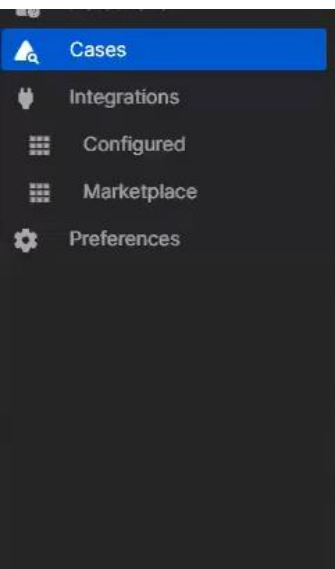
This credential has Write Access

☐ I have read and understood the information above and have granted the correct permissions. I understand the security implications of creating and using this credential.

XDR 偵測可以看到許多第三方資料

Time ▾	Entity ▾	Category ▾ 	Source ▲ 	MITRE Attack
11/10/23, 11:17 AM		Firewall	Palo Alto Networks	Defense Evasion
11/10/23, 11:17 AM		Firewall	Fortinet	Initial Access
11/10/23, 11:17 AM		Firewall	SonicWall	Exfiltration
11/10/23, 11:15 AM		Iam	ManageEngine	Persistence
11/10/23, 11:07 AM		Firewall	Fortinet	Execution
11/10/23, 11:07 AM		Firewall	Fortinet	Execution
11/10/23, 10:51 AM		Firewall	Fortinet	Initial Access
11/10/23, 5:30 AM	Webserver	Endpoint	Sophos	Execution

調査案例



<input type="checkbox"/>	High	3-211960	Investigating	xdr-for-cases-1111@sophos.com	Hello1	XDR	11/2/2023, 12:44:18 PM	11/10/2023, 10:50:20 AM	6
<input type="checkbox"/>	Critical	3-214867	New	shivani.g+xdr-actions@sophos.com	up	XDR	11/9/2023, 3:13:12 PM	11/9/2023, 3:14:17 PM	0
<input type="checkbox"/>	Critical	3-214866	New	shivani.g+xdr-actions@sophos.com	qwewqe	XDR	11/9/2023, 3:12:09 PM	11/9/2023, 3:12:09 PM	0
<input type="checkbox"/>	Low	3-213877	Investigating	ryanbreaksstuff+qaxdrcasesuser2@gmail1.com	New Allan and Me Updated	XDR	11/6/2023, 6:03:38 PM	11/8/2023, 9:52:47 AM	1
<input type="checkbox"/>	Info	3-211959	Investigating	xdr-for-cases-1@sophos.com	New info case	XDR	11/2/2023, 12:15:43 PM	11/2/2023, 12:15:43 PM	1
<input type="checkbox"/>	Critical	3-189714	Investigating	shivani.g+xdr-actions@sophos.com	WIN-PROT-VDL-MALWARE-ATK-ATOMICRED-A	XDR	9/22/2023, 1:08:30 PM	11/10/2023, 11:19:44 AM	24
<input type="checkbox"/>	Medium	3-189898	Investigating	xdr-for-cases-1@sophos.com	New case	XDR	9/25/2023, 2:06:31 PM	10/30/2023, 6:27:56 AM	6
<input type="checkbox"/>	Medium	3-210658	New	xdr-for-cases-1@sophos.com	New test case	XDR	10/30/2023, 6:10:03 AM	10/30/2023, 6:10:03 AM	0

案例摘要

Overview Detections Notebook History Respond

Summary

Various suspicious commands for looking to harvest credentials from the Server.

MITRE Tactic(s)

0 3 6 5 6 6 0 0 0 0 0 0

>	TA0002	Execution	3
>	TA0003	Persistence	6
>	TA0004	Privilege Escalation	5
>	TA0005	Defense Evasion	6
>	TA0006	Credential Access	6

Recent activity

- Oct 25, 2023 9:51:00 AM
xdr-for-cases-1@sophos.com status changed from "new" to "investigating", updated_at changed to "2023-10-25T16:50:59.992Z"
- Oct 25, 2023 9:51:00 AM
xdr-for-cases-1@sophos.com status changed from "new" to "investigating"
- Oct 25, 2023 9:51:10 AM
xdr-for-cases-1@sophos.com owner_email changed from "Unassigned" to "xdr-for-cases-1@2023-10-25T16:50:59.992Z" to "2023-10-25T16:51:10.551Z"
- Nov 10, 2023 11:17:47 AM
xdr-for-cases-1@sophos.com notes changed from "test summary" to "Suspicious commands"
- Nov 10, 2023 11:19:44 AM
xdr-for-cases-1@sophos.com notes changed from "Suspicious commands for Credentials" to "g to harvest credentials from the Server."





事件回應

look

History

Respond

All Actions

Name↑↓	Description	Categories	Vendor
Clear User Sessions	Removes all active identity provider sessions	Identity	 Okta
Expire Password	This operation transitions the user status to PASSWORD_EXPIRED so that the user is required to change their password at their next login.	Identity	 Okta
Unsuspend User	Unsusponds a user and returns them to the ACTIVE state	Identity	 Okta
Suspend User	Suspends a user	Identity	 Okta



Suspend User

Integration

RickC2

Manage Integrations

Username

jim@realod.com

Fully-qualified sign in name (for example: dade.murphy@example.com).

Reason

this is a compromised cred - needs to be disabled

Run



Return to Respond

Suspend User In Progress

Details

Created at 11/10/2023, 11:56:36 AM

Run by Administrator

Integration RickC2

Reason this is a compromised cred - needs to be disabled

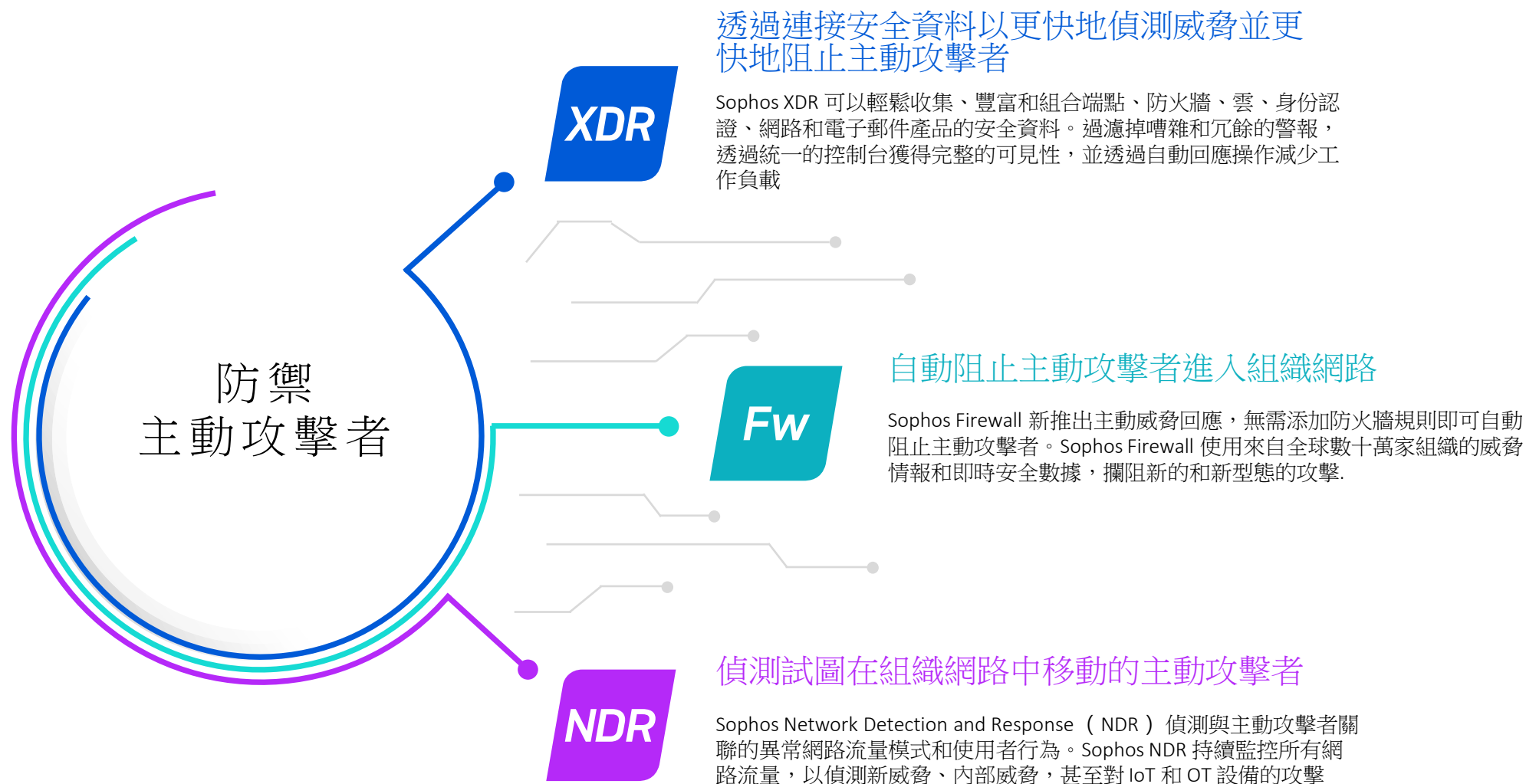
Inputs

Username jim@realod.com

Outputs

No outputs

NDR



Sophos NDR

熟練的攻擊者可以逃避偵測並刪除其存在的證據。但是他們需要在網路中移動才能進行攻擊。

Sophos NDR 可以看到防火牆和端點無法看到的行為和威脅



未防護的設備

保護不支援安裝端點防護的設備，例如 POS 系統、舊的作業系統、IoT 和 OT 設備



不明設備

使用網路設備尋找功能監控未知或未安裝防護設備



可疑的資料傳送

即時查看疑似正常的活動，例如在遠端連線期間緩慢上傳的資料



內部威脅

探知在非工作時間發送到異地理位置的網路流量

Sophos NDR 即時運行 5 個獨立的檢測引擎



5 個獨立的偵測引擎

DDA Device Detection Analytics

識別網路上不受 Sophos 管理的系統資料傳輸，包括未經授權的潛在惡意設備

DGA Domain Generation Algorithms

藉由利用深度學習長短期記憶（LSTM）預測模型，檢測演算法產生的網域

DPI Deep Packet Inspection

檢測加密和純文字流量中的已知IOC，以快速識別發動攻擊者和TTPs(攻擊模式或特徵)

SRA Session Risk Analytics

強大的邏輯引擎，利用針對基於連線階段的風險因子（例如，自己指定的 TLS 證書、二進位應用程式傳輸等）發出警報的規則

EPA Encrypted Payload Analytics

根據工作階段封包大小、方向和到達間隔時間中發現的模式檢測零時差 C2 伺服器 and 惡意軟體系列的新變種

NDR 與防火牆有何不同？

防火牆

- 監控進入和離開的內容
- 阻止不請自來和不需要的流量
- 回應主動威脅
- 無法瞭解內部網路上發生的情況



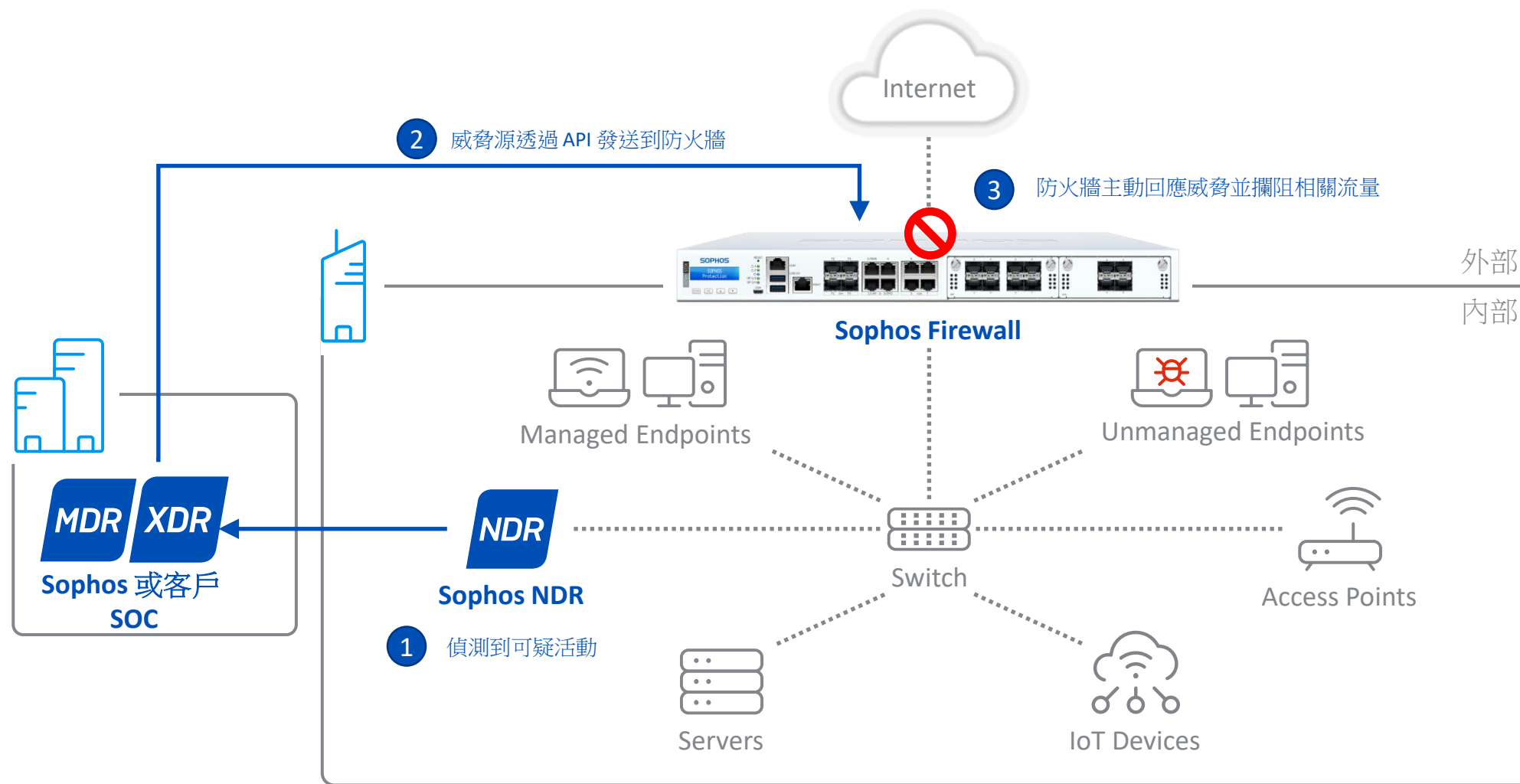
外部
內部

NDR

- 監控和分析內部網路內發生的情況
- 識別可疑或惡意活動
- 不控制網路流量



Sophos NDR 現在可用於 XDR



終極偵測和回應

