BROADCOM SOFTWARE

# Symantec Endpoint Security：

## SEP/SESE/SESC 端點安全三料號

# 業界最完整的端點安全解決方案

保安資訊-賽門鐵克決方案專家
https://www.savetime.com.tw

# 賽門鐵克企業市場滲透率


1. 財富前500大企業有**195**家
2. 全球前2000大企業有**697**家
3. 全球前13大銀行全都是
4. 全球前10大電信公司有**8**家
5. 全球前10大汽車製商有**7**家
6. 全球超過**1.5**億個企業用戶

BROADCOM SOFTWARE

# 關於博通賽門鐵克

- 博通賽門鐵克長期獲美國總統任命，成為美國國家安全通訊諮詢委員會(NSTAC)一員，也是目前唯四的資安廠商之一。能提供總統建言，為通訊與資訊科技重要基礎建設的安全和保護盡一份力量。
- 博通賽門鐵克也是唯一參與國際網路工程研究團隊的資安廠商(IETF:Internet Engineering Task Force)，IETF是一個開放性的國際組織，其作用在於匯集網路設計師、網路操作員、網路廠商以及研究人員共同研發改進網路的工程架構與建立起一個平穩的網路環境。例如：TLS1.3、ECH(Encrypted Client Hello)、DNS 以及HTTP……等。
- 博通賽門鐵克是開放網路安全模式框架(Open Cybersecurity Schema Framework，OCSF）專案創始成員之一，OCSF專案包含一個開放規格，以用來建立各種安全產品及服務之安全遙測的標準化資料，以及各種可支援及加速採用OCSF模式的開源工具，以協助組織更快也更有效率地偵測、調查與阻止網路攻擊。

# 關於我們


*服務電話:*

**0800-381-500**
**+886-4-23815000**

*網站:*

**www.savetime.com.tw**


# 保安資訊

## 從協助顧客簡單使用賽門鐵克方案開始到滿足顧客需求更超越顧客期望的價值

- 保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。
- 自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢，能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。
- 許多顧客樂意與我們建立起長期友誼，把我們當成可信任的資安建議者、可提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

BROADCOM SOFTWARE

# 賽門鐵克端點安全系列三料號比較 SESC ≧ SESE ≧ SEP

Symantec

| 防護系列 | 產品名稱 | SEP | SESE | SESC |
|---|---|---|---|---|
| 工作站防護 | Symantec Endpoint Protection 14.X for Windows 7/8(.1)/10/11/Macintosh-最新版 | 有 | 有 | 有 |
| 伺服器防護 | Symantec EndPoint Protection 14.x for WIN 2008R2/2012(R2)/2016 /2019/2022/ Supported Multi-Vendors Linux SERVER--最新版 | 有 | 有 | 有 |
| 中央集中控管 | 地端自建管理主控台--Symantec Endpoint Protection Manager 最新版(用戶端：Windows/Linux/Macintosh) | 有 | 有 | 有 |
| | 雲端管理主控台(支援用戶端：iOS/Android/Windows-s/Windows/ Linux/Macintosh) | | 有 | 有 |
| 行動裝置防護 | EndPoint Protection for iOS/Android/Windows-s--最新版(只支援雲端主控台控管)+安全連線檢查(SECURE NETWORK CONNECTION) | | 有 | 有 |
| EDR | Symantec Endpoint Detection & Response 端點偵測與回應 --支援地端/雲端管理主控台(有含雲端沙箱功能) | | | 有 |
| AD 防護 | Symantec Threat Defense for Active Directory.基於端點防禦技術的微軟 AD 威脅防禦--支援地端/雲端管理主控台 | | | 有 |
| Adaptive 防護 | 已內建於 SESC 標準功能(自適應防護)-智能型能的應用程式控管以及有效預防內建或第三方系統管理工具成為駭客的幫兇工具(就地取材攻擊) | | | 有 |

SEP ：Symantec Endpoint Protection-賽門鐵克端點防護(地端自建主控台)

SESE：Symantec Endpoint Security Enterprise-賽門鐵克端點安全企業版(雲端/地端主控台可依需求自行選擇)

SESC：Symantec Endpoint Security Complete--賽門鐵克端點安全完整版(業界最完善的端點安全完整組合--完整應對 MITRE ATT&CK 框架)




BROADCOM SOFTWARE

# 為什麼 Symantec Endpoint Security
# 是最完整的端點安全解決方案

Symantec

## 最深層的防護

次世代
防止偵測回應

盲點
適應 控制 驗證

防禦所有
攻擊媒介和方法

## 最廣泛的適用範圍

傳統平台

新式平台

運算和存儲

廣泛的適用範圍
保護所有端點

## 現代化的管理

ADAPTIVE
自動評估 → 自動建議

雲端 混合 地端

現代化管理&新式應用程式

透過現代化管理
擴展安全性

## 整合架構

簡化架構
單一代理程式
單一主控台

SYMANTEC 整合
WSS DLP ICA CASB

開放式平台
XDR OpenC2
MS Graph API

實現卓越的
運營效率

## 異質平台的同質端點安全與管理




BROADCOM SOFTWARE

# 業界唯一涵蓋完整 MITRE ATT&CK 攻擊鏈框架的創新防護技術集

| 攻擊前 | | 入侵 | | | | 感染 | | | 侵擾 | | | | 外滲 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 攻擊前 | | 初始訪問 | | | | 執行 | 持久化 | 提升權限 | 躲過/破壞防禦 | 帳密盜用 | 發現 | 橫向移動 | 資料收集 | 命令和控制 | 資料滲漏 |
| **安全漏洞評估** | **應用程式控管** | **維護連線安全** | **入侵預防** | **雲端信譽分析** | **進階機器學習** | **CP3 描述語言模擬器** | **漏洞利用防護** | **行為分析** | **竄改防護** | **欺敵技術** | **AD入侵防護** | | | **入侵預防** | |
| Threat Defense for AD會使用攻擊模擬技術持續探測網域的不當組態、漏洞及持續性，並由攻擊者觀點向Active Directory管理員呈現其網域狀態，以便立即緩和風險減少攻擊面 | 透過僅允許執行已知安全的 / 經授權的應用程式或限制存取登錄檔，將端點攻擊面減至最少，進而強化對進階攻擊的防禦 | 可識別惡意 Wi-Fi 連線，提供政策導向 VPN，以保護網路連線(中間人攻擊)及支援合規性 | 攔截利用已知漏洞的攻擊 | 利用賽門鐵克用戶及安全相關社群的集體智慧，來評比檔案或網頁的安全等級 | 藉由預先執行並偵測與分析程式碼的的惡意特徵，特別有利於發現新型態及不斷突變的威脅 | 藉由預先執行並偵測與分析描述語言相關的威脅，例如VB、Java、Powershell…等。 | 攔截零時差或未知型漏洞攻擊 | 記錄與分析端點行為來識別進階攻擊戰術與技術，偵測偽裝成合法使用者卻執行異常活動的攻擊者。包含Non PE以及執行DLL側載 (DLL Side-Loading) | 預防惡意程式或人為破獲，停用或破獲安全軟體正常運行 | 使用誘騙和誘餌(如假檔案、假憑證、假網路共享、假快取項目及假端點)的主動式安全功能，欺騙攻擊者進入而讓自己曝光與其攻擊目標，能夠揭露並延誤攻擊者的行為 | 在端點結合AI、模糊和進階鑑識方法來因應各種秘密攻擊或APT，以提供自動入侵遏止、資安事端回應及網域安全評估等功能。這是唯一安全解決方案，能在攻擊者入侵端點後加以遏止，不會讓攻擊者存留在網域中。本解決方案可中斷偵查活動、防止憑證竊取、避免攻擊者利用Active Directory橫向移動至其他資產 | | | 攔截對外連線惡意命令和控制主機(C&C)，避免資料外洩及阻斷加密勒索攻擊活動中的密鑰遞交交握連線 | |

**自適應(Adaptive)保護**：深入洞見威脅態勢 | 自訂行為洞見 | 矯正

**偵測與回應**：系統運行記錄功能 | 行為鑑識 | 目標攻擊雲端分析 | 威脅獵手分析

**全球情報網路(GIN)**：每天數十億次的查詢賦予完整的保護與偵測能力

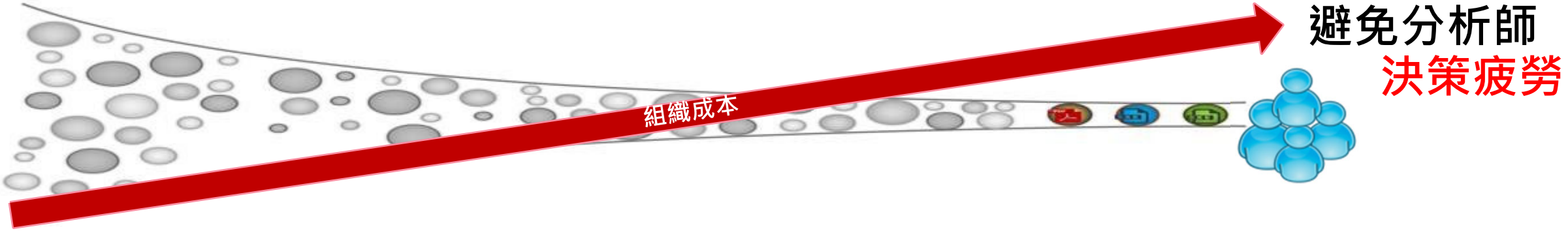
**整合式網路防禦 (Integrated Cyber Defense) 平台**：
可與賽門鐵克及第三方資安與事件管理系統(SIEM)/威脅情報平台(TIP)/ 資安協調自動化與回應(SOAR)整合




BROADCOM SOFTWARE

# Symantec Endpoint Security-不斷創新、超越自我，領先業界

| 攻擊前 | 入侵 | 感染 | | | 侵擾 | | | | 外滲 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 攻擊前 | 初始訪問 | 執行 | 持續性 | 權限提升 | 躲過/破壞防禦 | 帳密盜用 | 搜索 | 橫向移動 | 資料收集 | 資料滲漏 | 命令和控制 |




## 攻擊面降低

- 入侵評估
- Adaptive 安全性
- 裝置控制
- 應用程式控制
- 自訂應用程式行為

## 入侵預防

- AD 威脅偵測
- 網路防火牆
- 入侵預防
- 安全連線
- 主機完整性

## 攻擊預防

- 惡意軟體防護
- 信譽分析
- 漏洞利用防護
- 模擬器
- 基於行為的預防
- 進階機器學習

## 偵測與回應

- 攻擊分析
- 行為鑑識
- SOC調查專家
- 威脅獵手專家團隊
- 快速回應

**單一代理程式** – 所有作業系統： Windows, Mac, Linux, Windows S Mode, Android, and iOS – 包含伺服器

**全球情報網 (GIN)** – 世界上最大的民用網路情報網




BROADCOM SOFTWARE

保安資訊 SAVETIME INFORMATION SECURITY

# Symantec Endpoint Security 如何保護您

## 賽門鐵克全球威脅情資

-- 推動世界級的檢測和保護力的**重大關鍵**

**9.0+**
PB(1PB=1024TB)
威脅態勢可見性

**5,000億**
為人工智慧驅動的情資圖譜創造優勢

**60億**
數位簽章相關特徵

**2,200萬**
行動裝置相關特徵

**20億**
可疑檔案

**460億**
網址記錄

**5億**
程序行為分類

## 從數字上來看

-- 無與倫比的可見性、檢測、保護

**0.8+**
十億
威脅被阻止

**45,432,000+**
惡意網頁重定向嘗試被阻止

**3,706,300+**
未知和 0-day 攻擊被阻止

**1,887,700+**
就地取材威脅被阻止

**1,182,800+**
勒索軟體 攻擊被阻止

**677,100+**
Powershell 攻擊被阻止

**142,500+**
AMSI 事件被阻止

## 人工智慧驅動的多層次防護

-- 深度防禦

### 入侵防禦
制敵機先 --
在攻擊到達端點之前阻止攻擊
基於入侵防禦

### 檔案檢查
透過進階機器學習阻止零日(0-Day)威脅
基於檔案檢查

### 行為安全
阻止
就地取材威脅
基於行為安全


以上數據為2022年4月的數據

保安資訊 SAVETIME INFORMATION SECURITY

# Symantec Endpoint Security (SES)

## 擁有50多項技術，可在整個 MITREATT & CK 規範的攻擊鏈中提供保護和檢測

### 入侵防禦技術

入侵防禦自動檢測並阻止網路攻擊和瀏覽器攻擊。賽門鐵克的入侵防禦技術是一流的深層封包檢測(DPI；Deep Packet Inspection)引擎，可保護數以千萬計的端點，包括《財星》500大企業和消費者。入侵防禦技術是賽門鐵克緊接在防火牆之後的第一道防線，為用戶端電腦和伺服主機提供保護。

- 每天在威脅獲得初始存取權限和／或執行執行之前，入侵防禦可以保護約70%到80%的所有攻擊，從而防止威脅對端點造成的入侵。
- 上個月阻止513+百萬次漏洞利用攻擊。
- 超過2.4+百萬個端點的803+百萬次攻擊中有96%在網路邊界就被阻止，從而防止威脅對端點造成的入侵。其餘4%的出埠流量被阻止，切斷與指揮和控制(C&C)的通信。
- 超過132+千台伺服器的105+百萬次攻擊中有93%在網路邊界被阻止，從而防止威脅對伺服器造成的入侵。其餘7%的出埠流量因切斷與指揮和控制的通信而被阻止。

### 檔案檢查技術

從檔案開始在端點下載的那一刻起，一整個完善的多重技術檔案檢查機制就能檢測和阻止惡意檔案。賽門鐵克密切監控威脅態勢，並採取主動措施來訓練和發布機器學習模型、模擬器和其他內容。該內容為許多威脅家族提供零日預防和啟發式檢測，以及未來可能重新出現的相關威脅。Symantec Endpoint Security能夠運行可攜式可執行檔(PE)和非PE模擬器來處理複雜的封裝工具、混淆程序等，如果允許這些惡意程式在端點的本機上執行，則後續難以遏制其後患無窮的破壞。

- 阻止3.7+百萬次威脅~透過經過訓練以防止零日攻擊的進階機器學習(AML)的結果。
- 上個月阻止70+千個多個基於x86的混淆惡意軟體的自定義加殼程序（例如：Lokibot）。
- 阻止142+千個AMSI事件~代表對終端和最終使用者的資料、應用程式和工作負載的使用者帳戶控制、PowerShell、Office VBA、JavaScript、VBScript和同樣的惡意軟體保護。
- 上個月阻止691+千次基於腳本和Powershell的攻擊，例如：Pandex、Emotet和LemonDuck。

### 行為安全技術

賽門鐵克的行為安全技術會監控端點上所有相關活動，了解正常的應用程序行為模式，並迅速發出警報或阻止偏離規範的行為。攻擊者不再使用通用攻擊工具，而是根據企業環境本身存在的管理或系統工具來定制攻擊。行為技術對命令行檢測、顯示可疑行為的應用程序行為（包括：非PE、DLL和側載）非常有效。

- 上個月，行為安全技術阻止1.4+百萬個威脅。
- 來自Conti、Emotet和Ryuk等所有勒索軟體家族的1.1+百萬次勒索軟體（和勒索軟體前導程式）活動以及使用Cobalt Strike等工具發起的攻擊都被行為安全技術阻止。
- 1.8+百萬次被阻止是利用現有工具（例如：PowerShell）的就地取材攻擊。

## 這對您的企業意味著什麼?

對您的SEP託管端點運行運行狀況檢查，以評估和優化您的安全狀況。

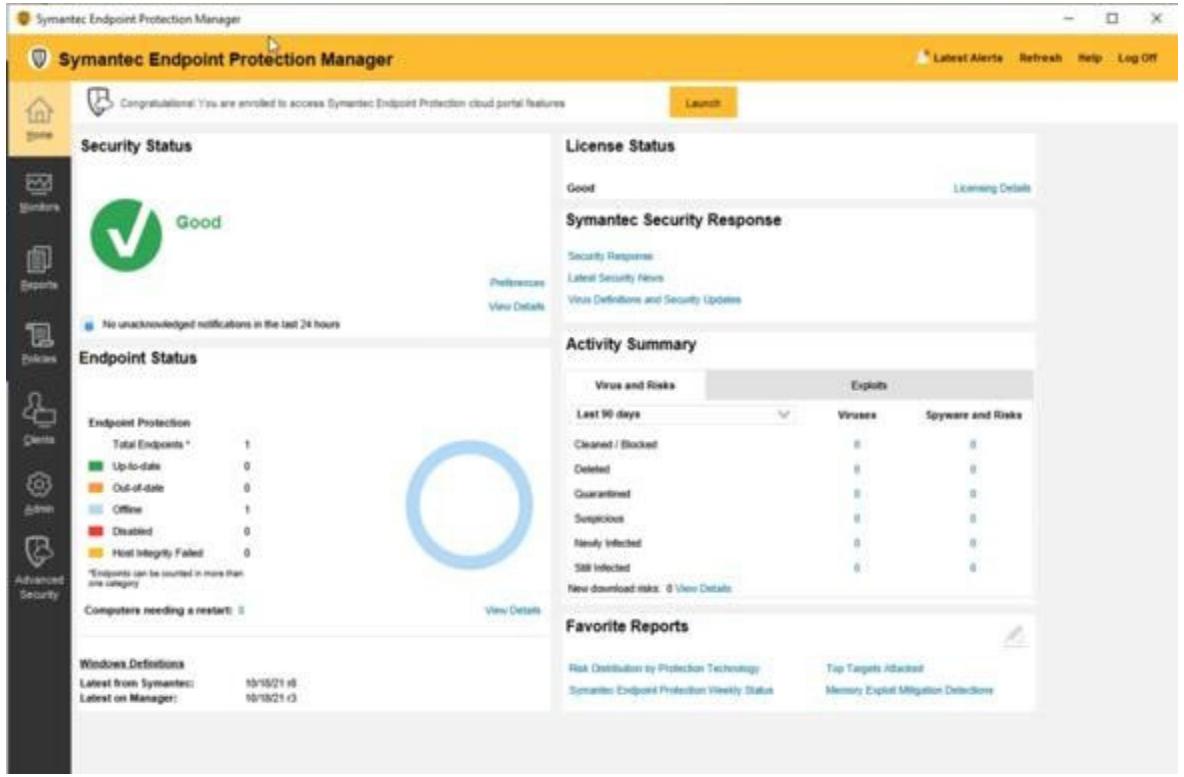
# 我們已經準備好迎接...

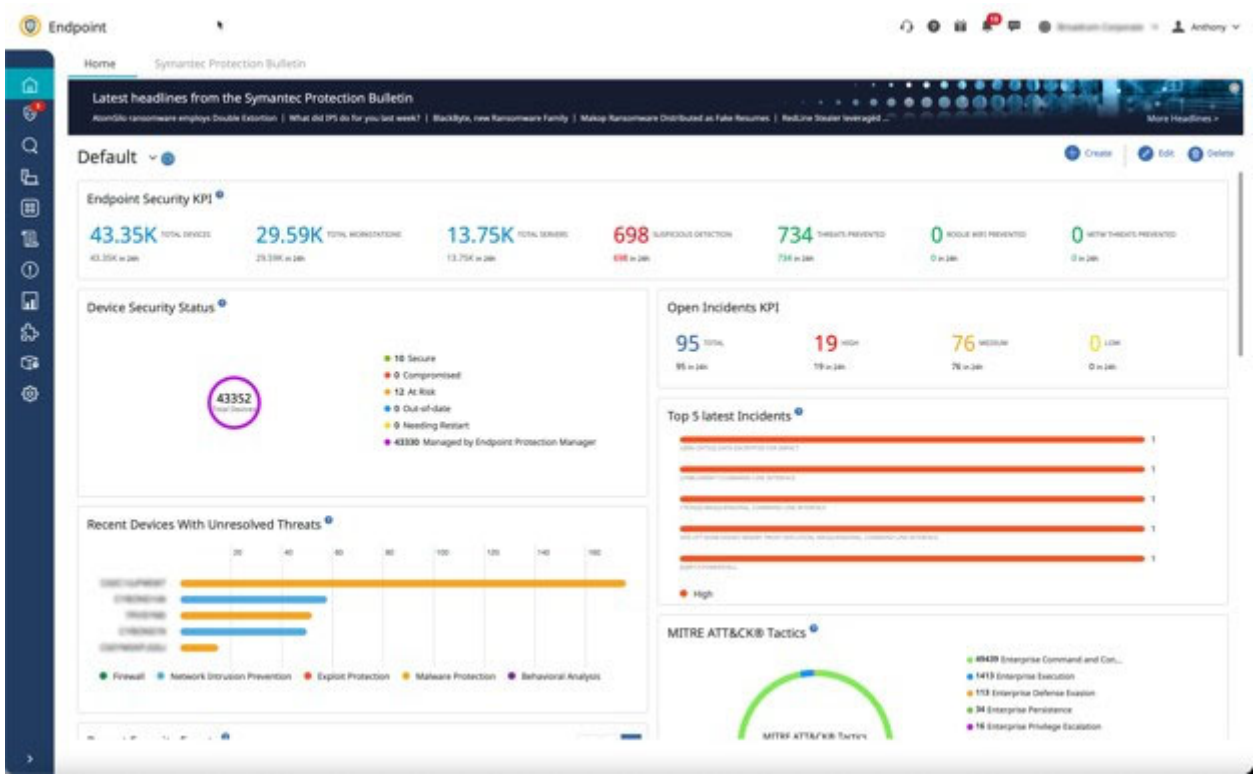
- 雲端移轉
- 提升防護能力



BROADCOM SOFTWARE

# 端點安全的旅程
# 轉移到雲端



BROADCOM SOFTWARE

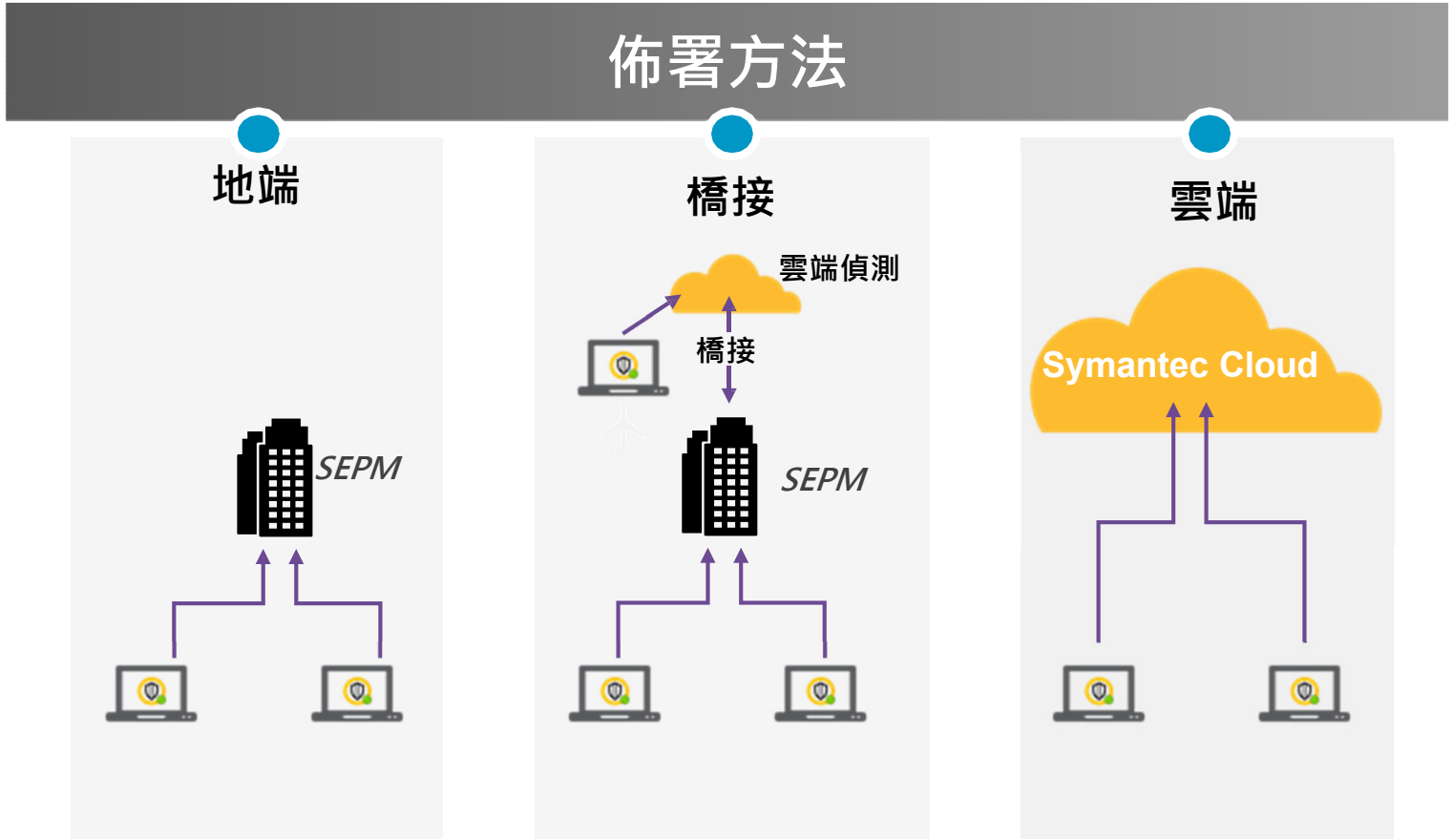
# 管理平台相容性比較

| | | | 地端 | 雲端 |
|---|---|---|---|---|
|  | 作業系統 | 工作站 (Windows/Mac) | ✓ | ✓ |
| | | 行動裝置 (iOS/Android) | | ✓ |
| | | 伺服器 (Windows/Linux) | ✓* | ✓ |
|  | 攻擊預防 | 惡意軟體防護 | ✓ | ✓ |
| | | 漏洞利用預防 | ✓ | ✓ |
| | | 防護強化 | | ✓ |
| | | 安全連線 | | ✓ |
|  | 攻擊面降低 | 安全漏洞評估 | ✓ | ✓ |
| | | 應用程式控制 | | ✓ |
| | | 自訂應用程式行為 | ✓ | ✓ |
| | | 裝置控制 | ✓ | ✓ |
|  | 防止入侵 | 入侵預防 | ✓ | ✓ |
| | | 防火牆 | ✓ | ✓ |
| | | 偽裝 | ✓ | ✓ |
| | | Active Directory 安全性 | ✓ *(2 主控台) | ✓ |
| | | 主機完整性 | ✓ | ✓ |
|  | 自適應 (Adaptive)保護 | Adaptative | 僅可檢視<br>需 ICDM | ✓ |
|  | 回應與矯正* | 系統運行記錄功能 | ✓ | ✓ |
| | | 行為鑑識 | ✓ | ✓ |
| | | 威脅獵手(Threat Hunter) | ✓ | ✓ |




BROADCOM SOFTWARE

# Symantec Endpoint Security | 佈署方法



# 輕鬆前進雲端管理的捷徑

## 無需新代理即可輕鬆從地端升級到雲端


1 端點上的相同 Symantec 代理程式

完整支援地端、雲端與混合模式

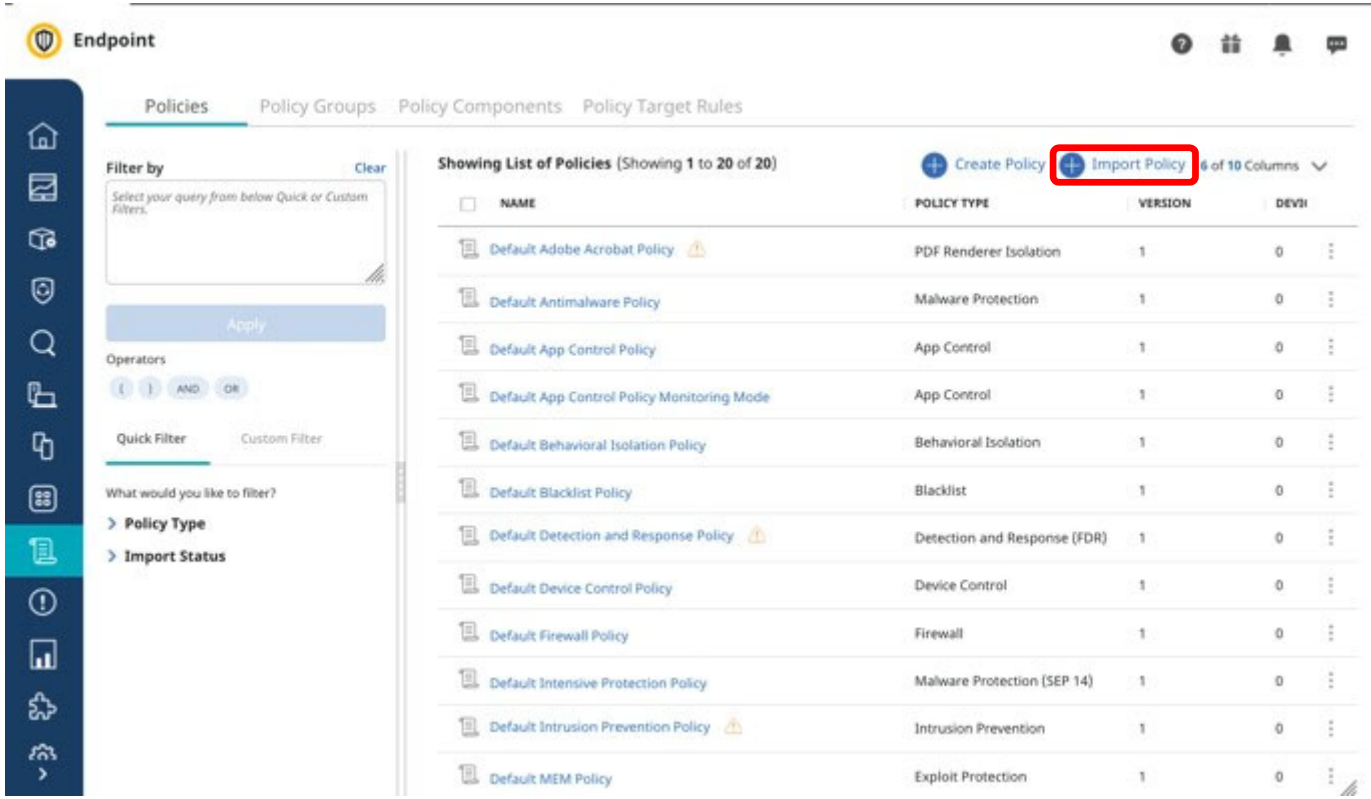



BROADCOM SOFTWARE

# 簡單就從地端 SEPM 管理主控台匯入政策

## 從SEPM匯出政策


## 開始匯入政策程序

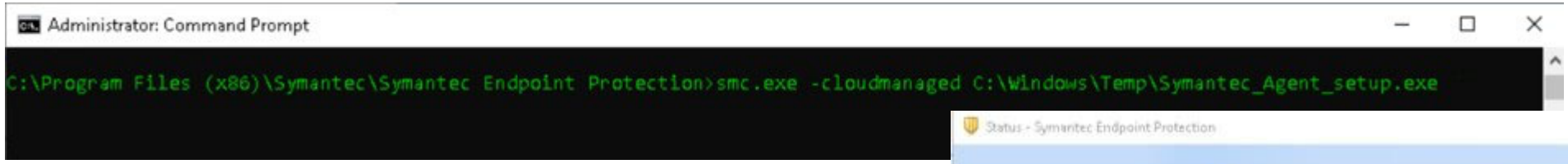


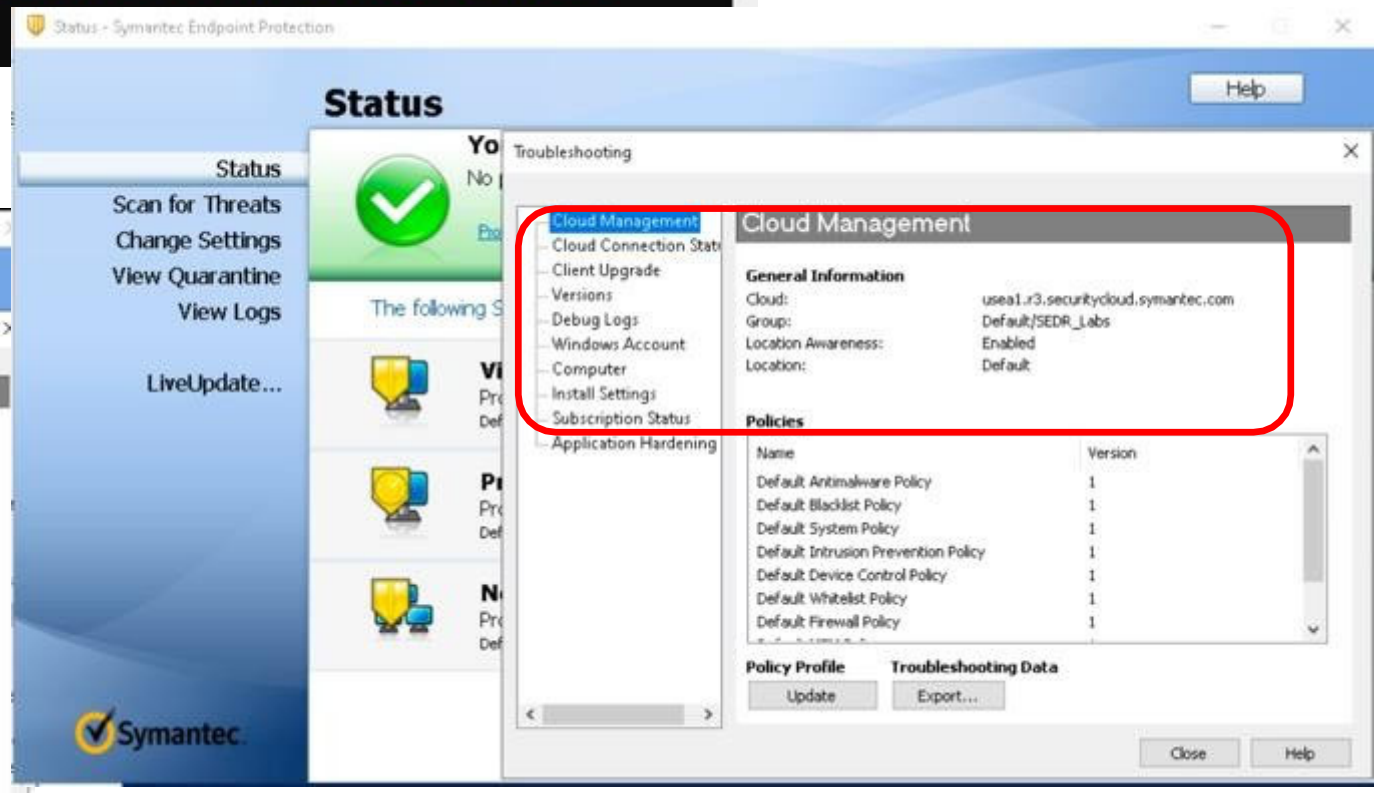
BROADCOM SOFTWARE

# 受地端 SEPM 管理的 SEP 移轉

- 將安裝套件派送到每個端點，然後執行 smc 命令列參數：




- SEP 用戶端重定導向到雲端受管理，
  無需重新開機或使用者互動。

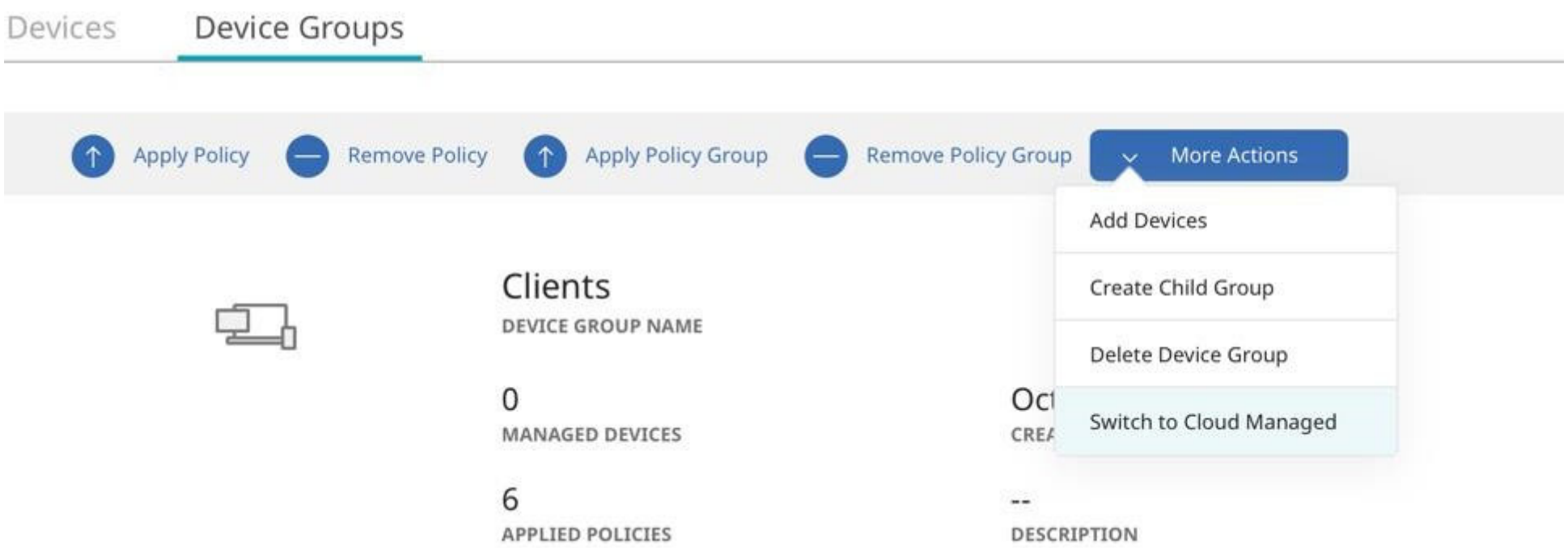




* Cloud Managed migration with SMC Command supported as of 14.2 RU1

BROADCOM SOFTWARE

# 新的移轉工具
# 即將推出



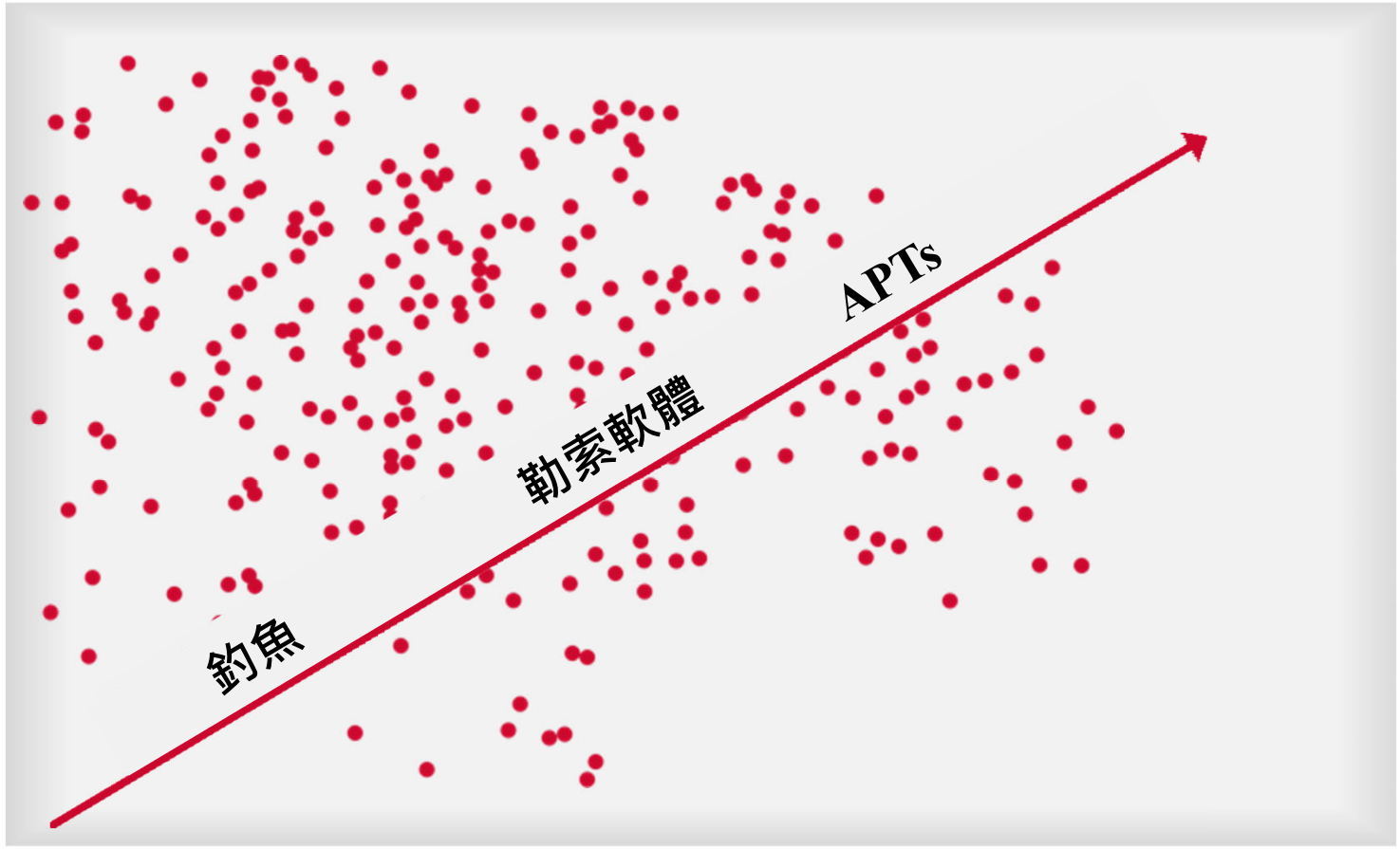

 

BROADCOM SOFTWARE

# 資安旅途中可以運用的導覽圖
# 讓你不再偏離既定的方向或是走入沒有成效的叉路

BROADCOM SOFTWARE

# 因應不斷演變的網路威脅，端點防護也需與時俱進




**2,000%**

兩用應用程式的惡意利用增加

**80%**

iOS 和 Android 漏洞增加

**62%**

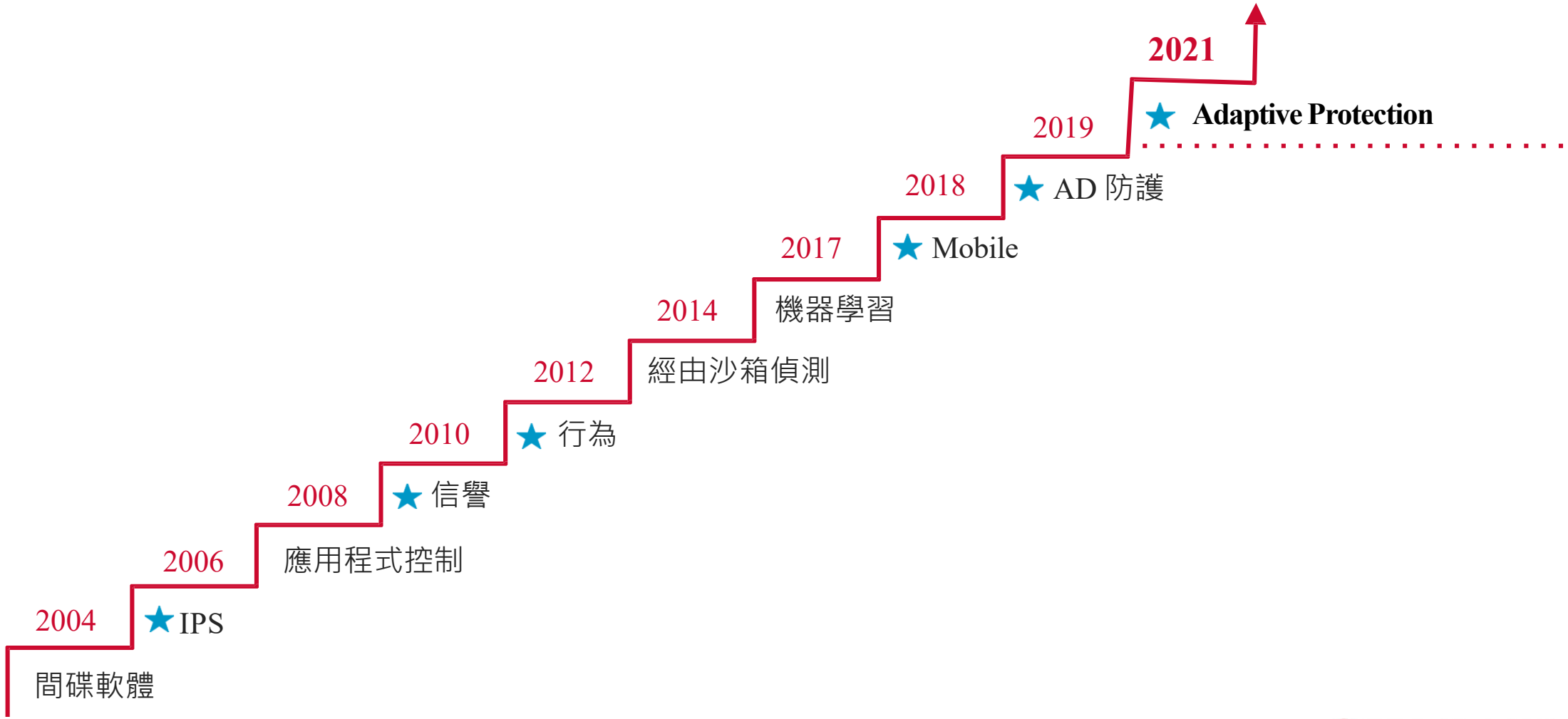
企業的針對性勒索軟體增加

BROADCOM SOFTWARE

# 防護旅程

## 因應不斷演變的網路威脅，不斷快速開發出各種創新解決方案



BROADCOM SOFTWARE

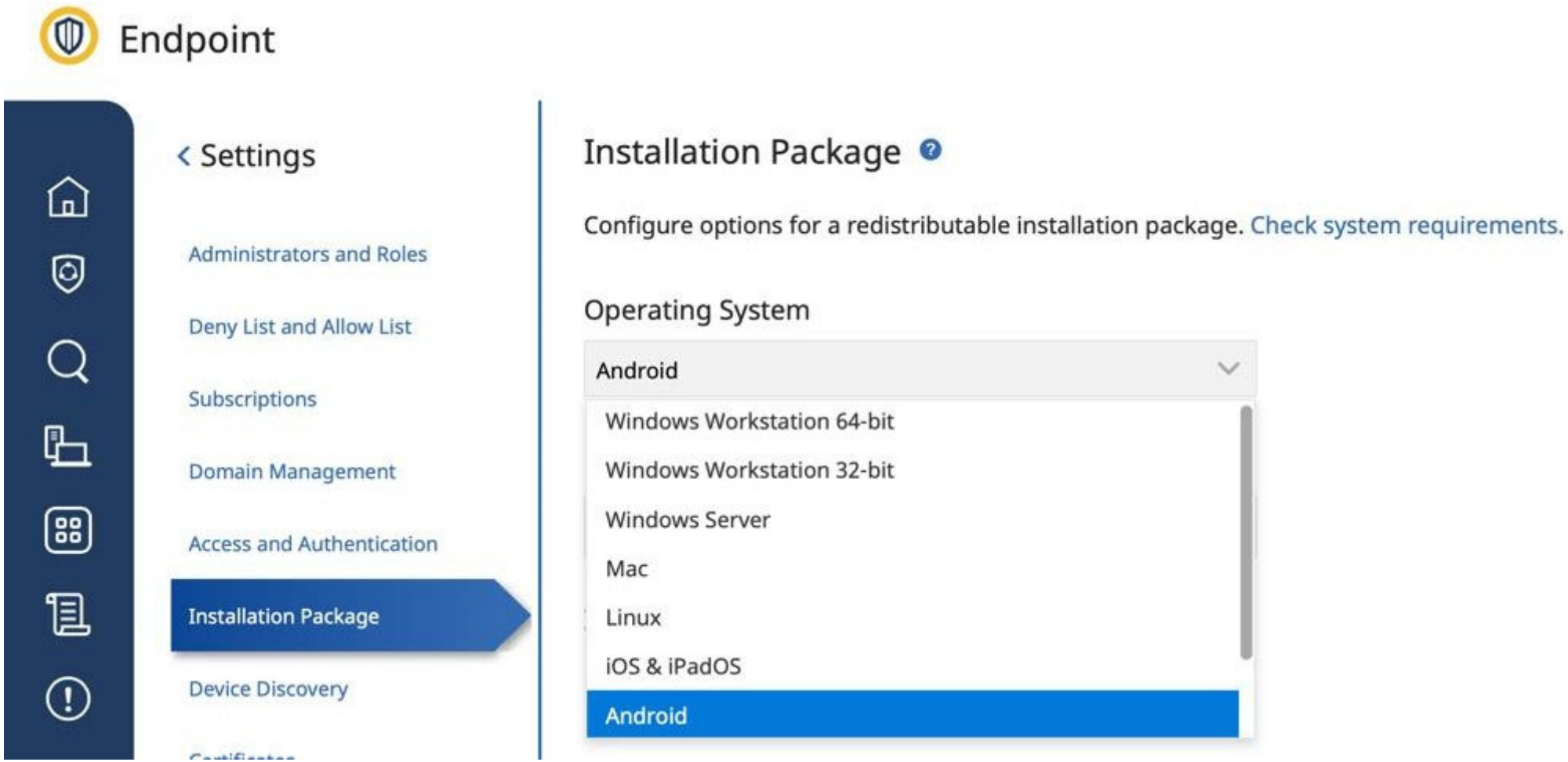
# 最近勒索軟體攻擊中最常見攻擊戰術流程(TTP；工具、策略和程序)

| MITRE | Top TTPs (Tactics, Techniques, and Procedures) | SES主動保護 |
|---|---|---|
| **Incursion 入侵** | IceID – email->maldoc->Powershell->cmd | • 程序歷程防護 |
| **Execution 執行** | IceID – dropper | • 檔案信譽 |
| **Command and Control命令與控制** | SystemBC – 遠端管理工具<br>Weirdloop – HTTPS stager | • 惡意網路通訊協定檢查 |
| **Privilege Escalation 權限升級** | CobaltStrike – GetSystem<br>Nsudo – UAC bypass, token impersonation | • 權限升級防護 (SONAR) |
| **Defense Evasion 回避防禦** | Disable MS Defender –<br>Powershell Set-MpPreference DisableRealtimeMonitoring | • Powershell 模擬器<br>透過Symantec防篡改功能讓SEP不能被停用 |
| **Credential Harvesting 憑證採集** | Lsass dump<br>Mimikatz, procdump | • Lsass 防護 |
| **Discovery 搜索** | Netscan –搜索開啟的 Web、檔案、資料庫伺服器和 RDP<br>Adfind – 列出使用者、電腦、網域和 DCs | • 兩用工具防護 |
| **Lateral Traverse 橫向移動** | PsExec | • 命令列檢查 |
| **Exfiltration 滲漏** | rclone – 大量檔案同步到雲端 | • 兩用工具防護<br>• 網路信譽 |
| **Impact 影響** | Ryuk, Sodinokibi – 加密 | • 檔案信譽<br>• 檔案加密機器學習 |




BROADCOM SOFTWARE

# 廣泛的平台支援



BROADCOM SOFTWARE

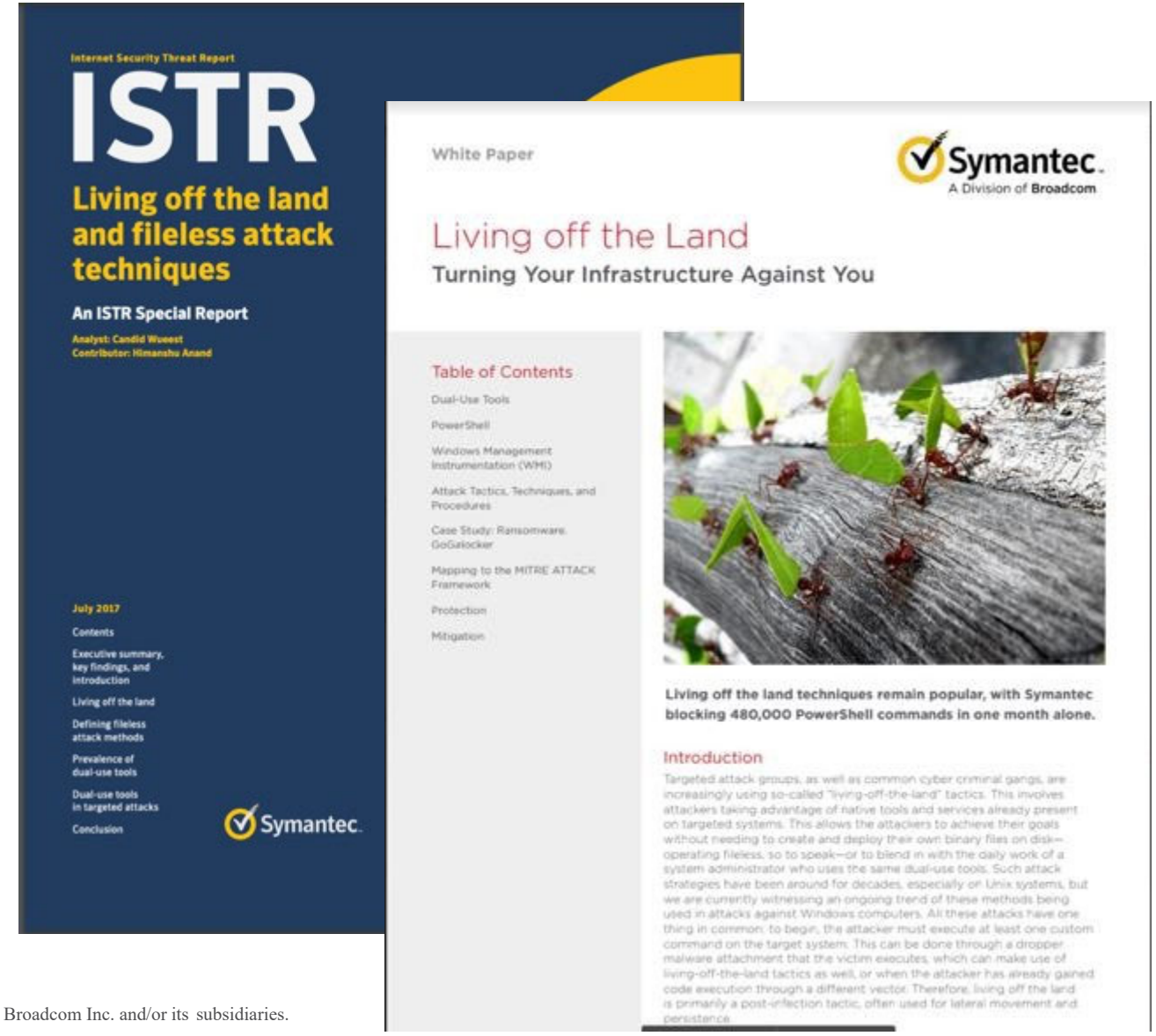
# Adaptive--自適應安全性

BROADCOM SOFTWARE

# 趨勢

# LotL

## Living off the Land
## 就地取材--
## 好工具被拿來當壞凶器



# 前十大兩用工具

| | |
|---|---|
| 1 | PowerShell |
| 2 | schtasks.exe |
| 3 | BITSAdmin |
| 4 | net.exe |
| 5 | PsExec |
| 6 | WMI |
| 7 | Certutil |
| 8 | cURL |
| 9 | Wget |
| 10 | tasklist.exe |




BROADCOM SOFTWARE

# Adaptive Protection | 防護就地取材攻擊

## 潛在攻擊路徑


**啟用 Adaptive：**

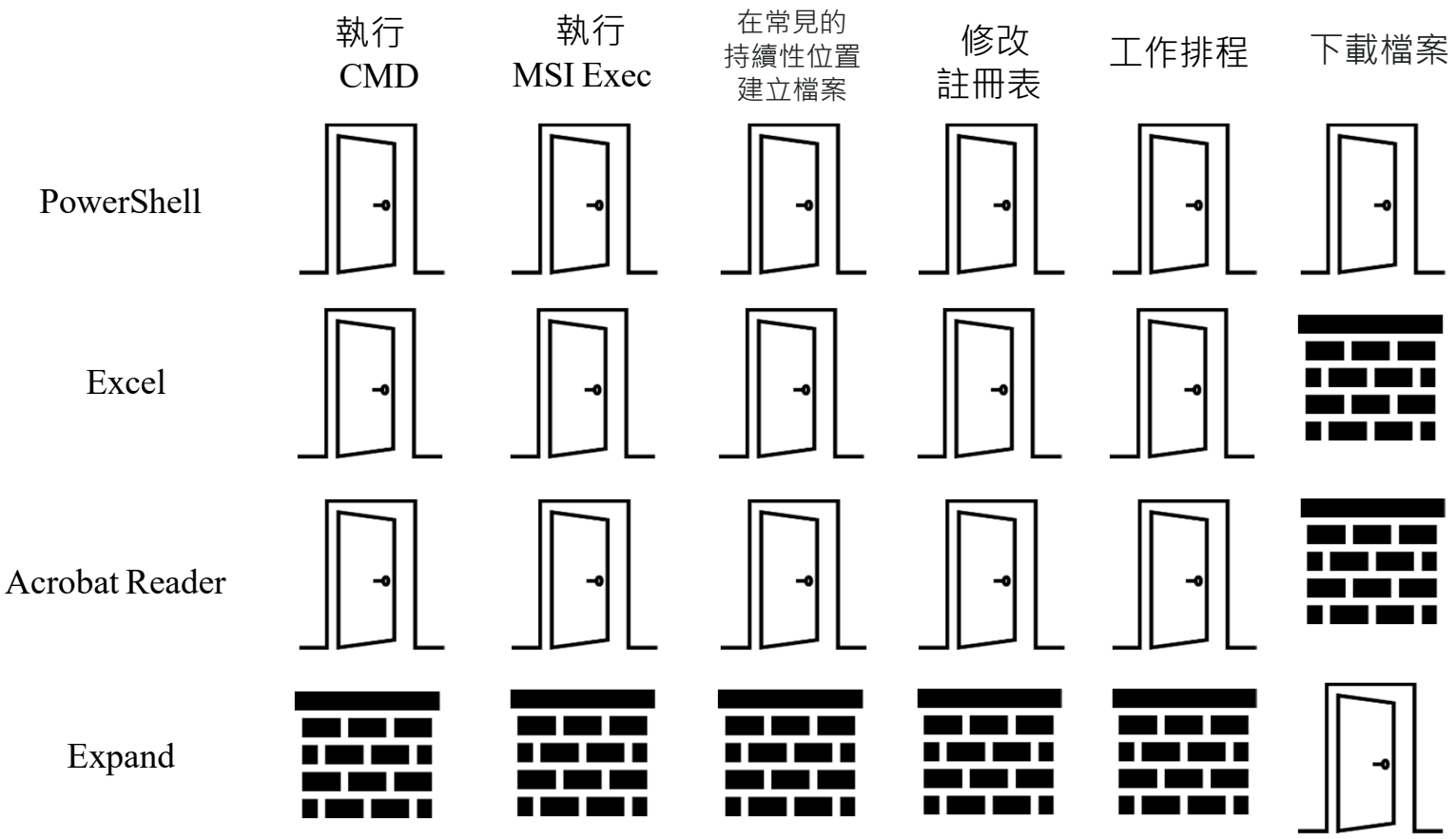
- 可完全針對個別環境打造的威脅預防戰術。
- 企業能夠**適應並調整**企業所需的預防新規則與條件
- 駭客入侵後的**橫向移動**將**日益困難**，有效遏止遍地開花攻擊災難




BROADCOM SOFTWARE

# 兩用工具

## 預設開放使用的風險等級




= 增加風險




BROADCOM SOFTWARE

# 兩用工具

## 明確的禁用策略


=

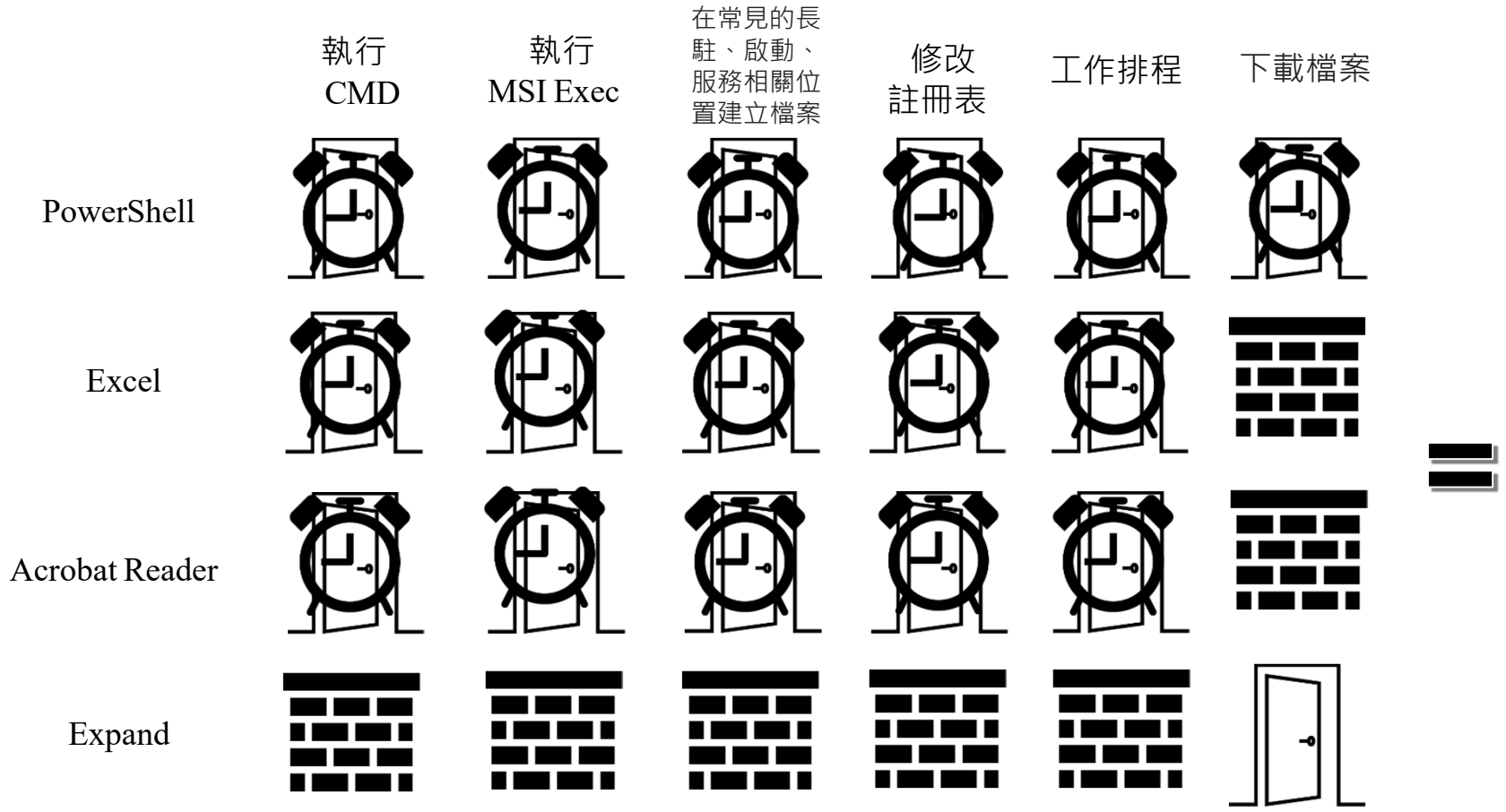
## 生產力減少




BROADCOM SOFTWARE

# 兩用工具

## 單靠 EDR 解決方案




**安全分析師干擾雜訊增加**

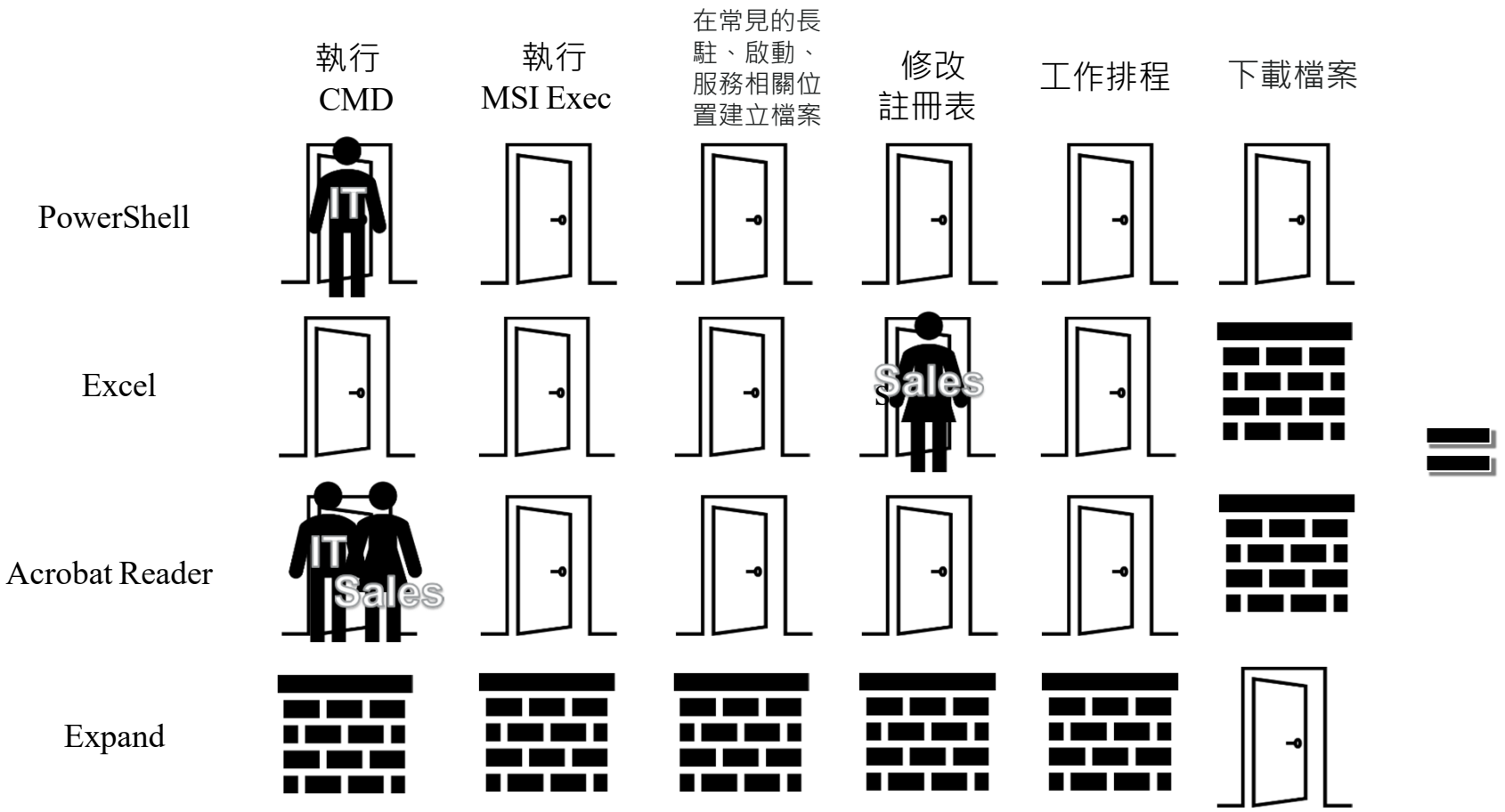
**被動回應**

BROADCOM SOFTWARE

# 兩用工具

## Adaptive 解決方案 – 瞭解正在使用工具的情境




**沒有減少生產力或造成影響**

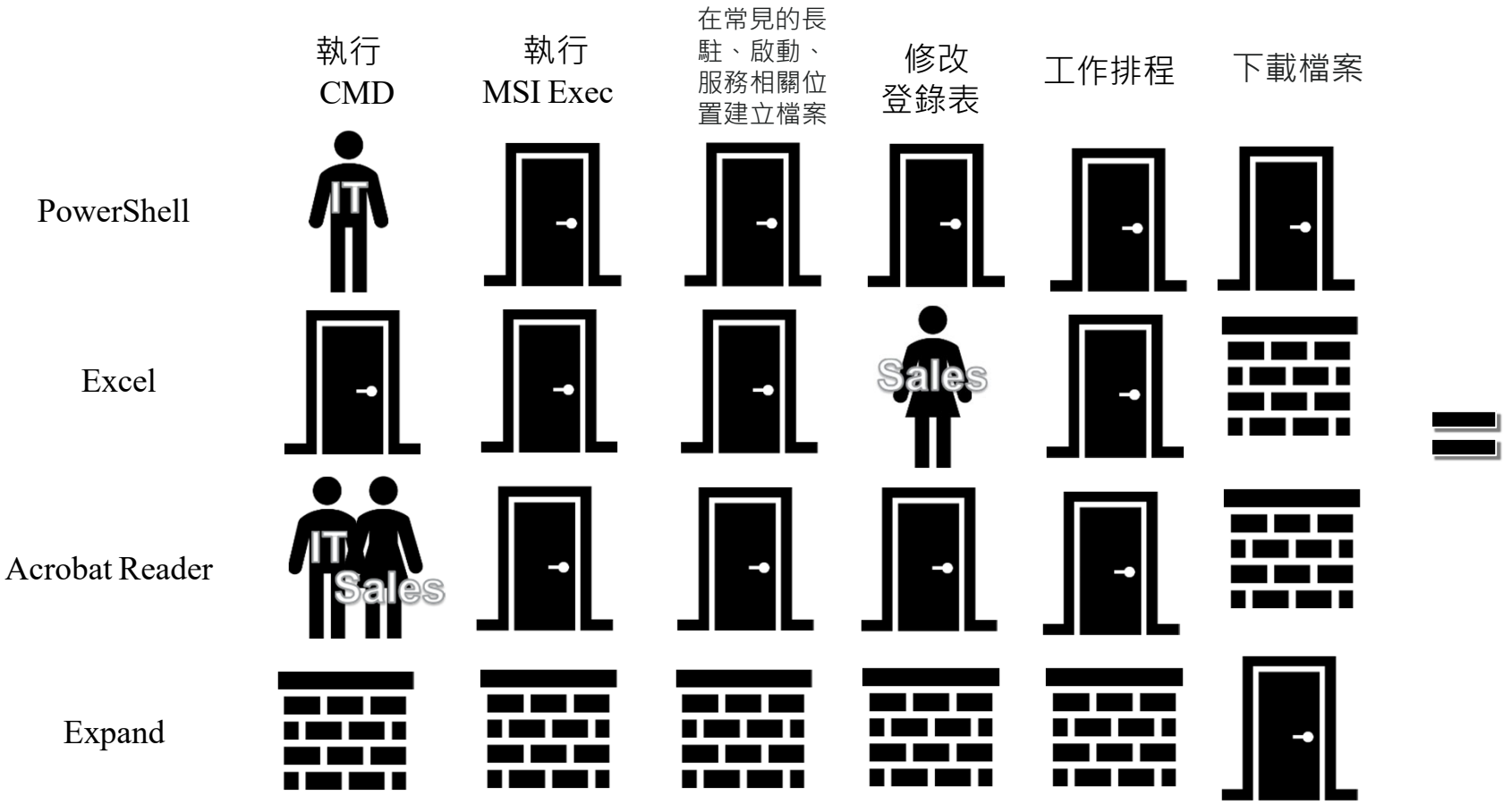
**使用最近90天的遙測數據**

BROADCOM SOFTWARE

# 兩用工具

## Adaptive解決方案 – 減少攻擊面



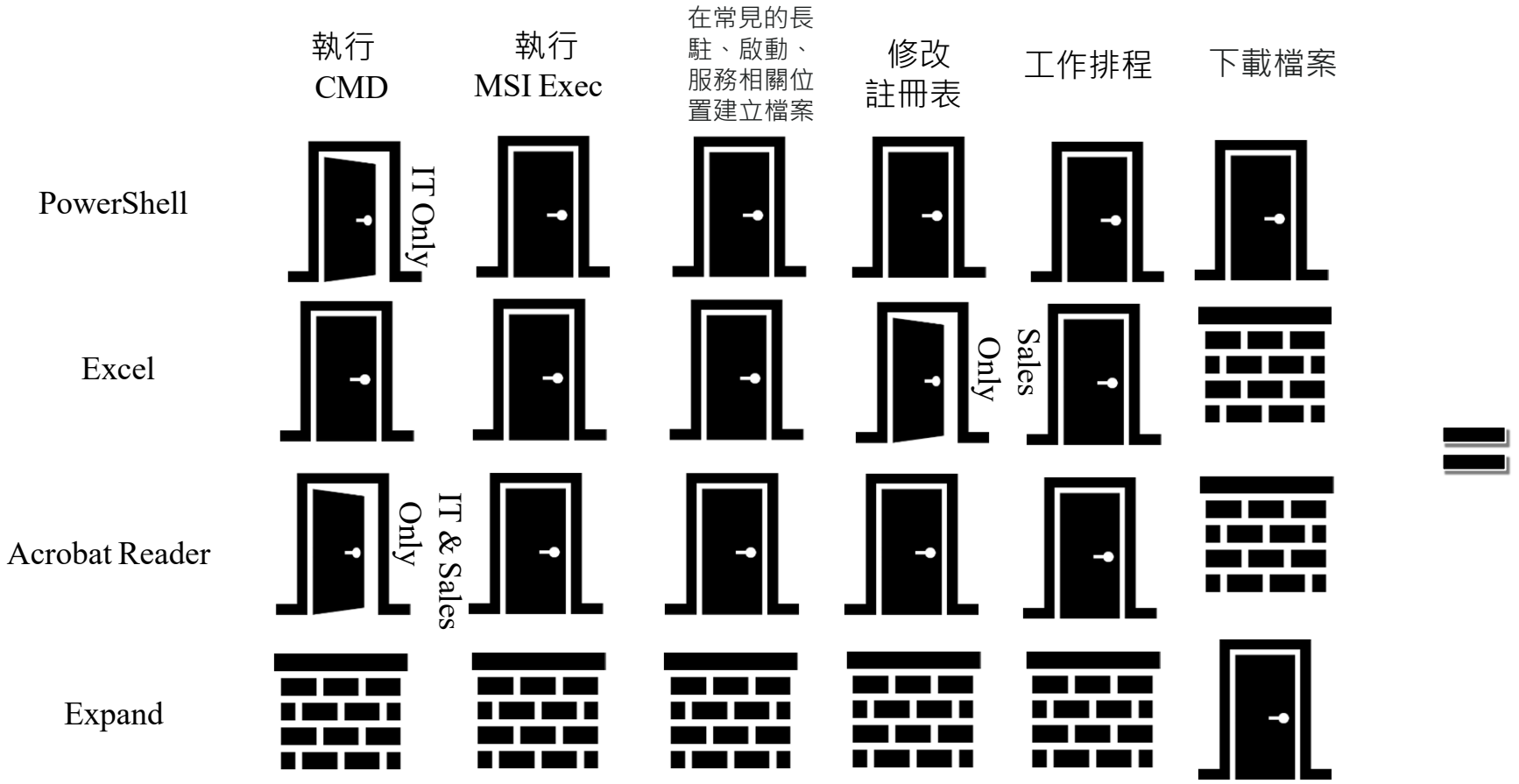

**已內建快速調整的選項**

BROADCOM SOFTWARE

# 兩用工具

## Adaptive解決方案 – 適應化修改 – 可微調




=

**縮短現有狀態與理想狀態之間的差距**

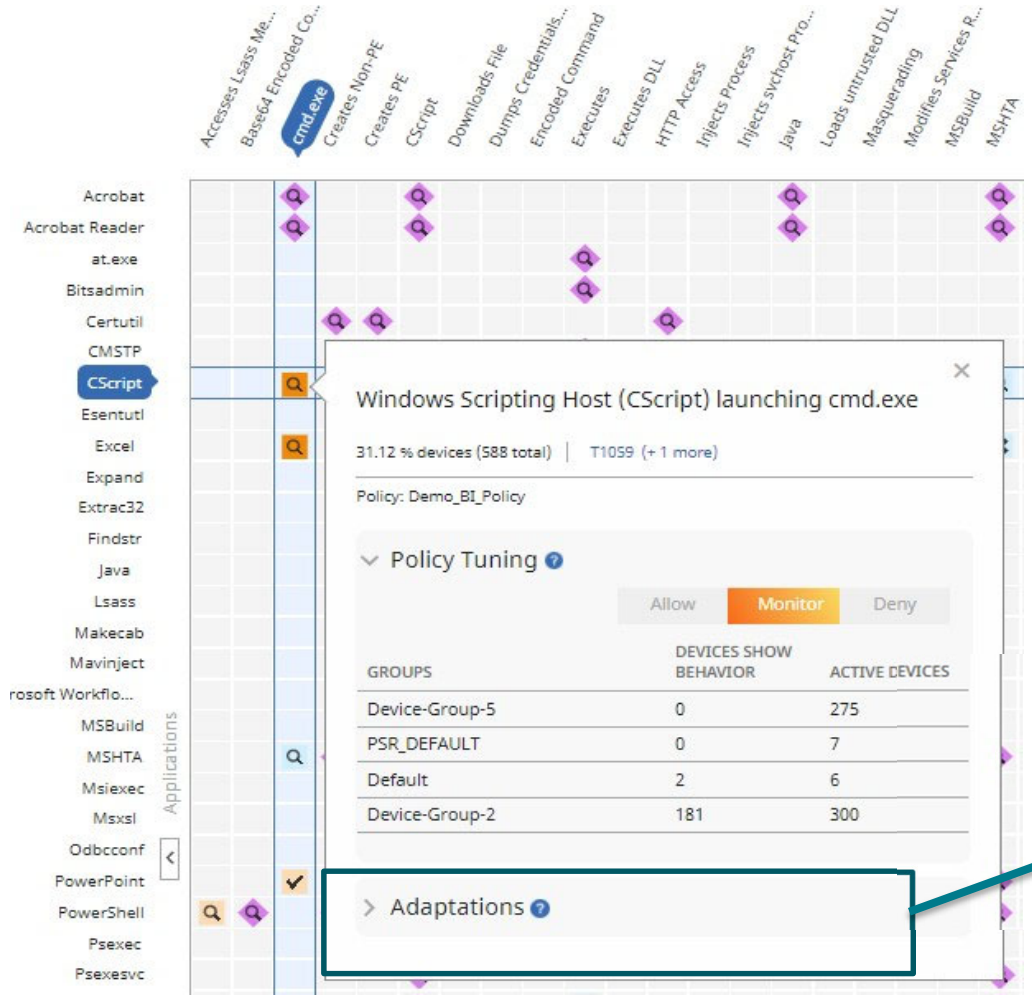


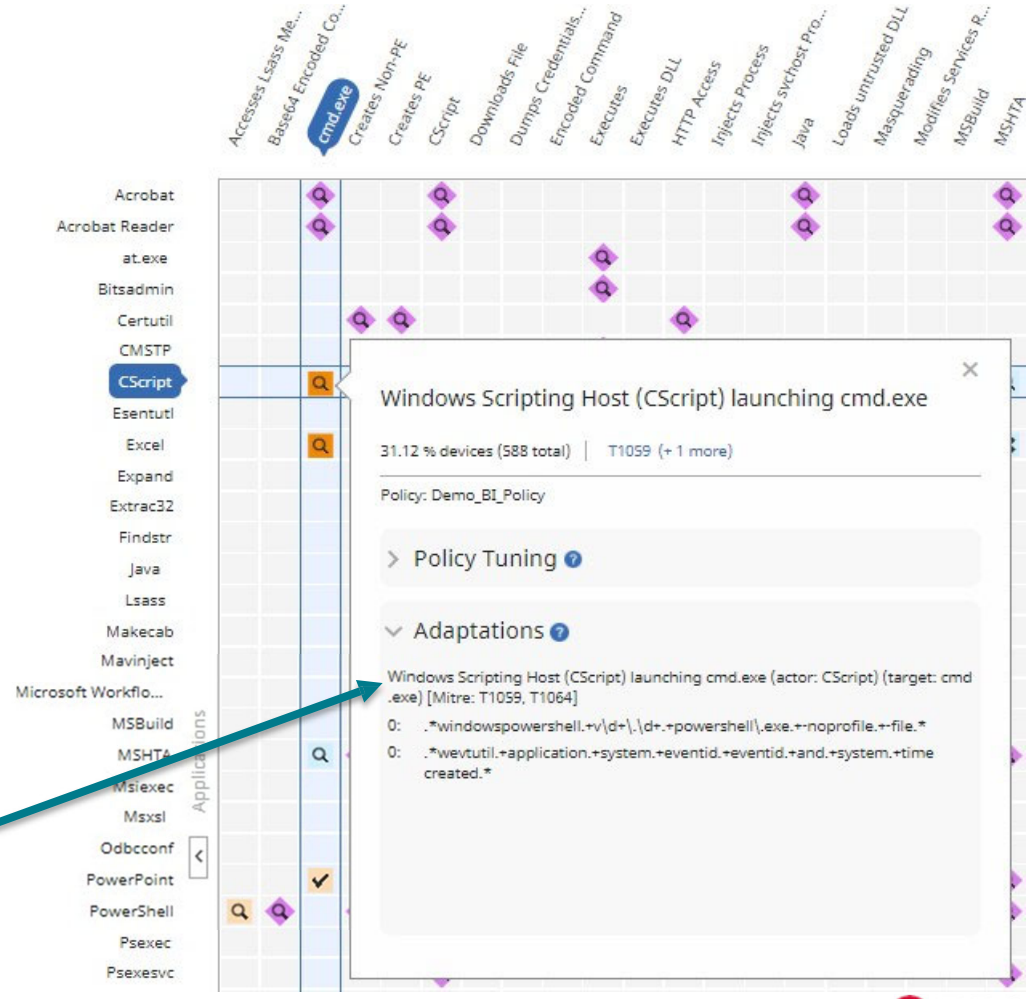

BROADCOM SOFTWARE

# Adaptive Protection | 適應化修改

## 優化攻擊面降低

*適應化修改透過排除良性行為將更多的行為規則從監控變更成攔截*



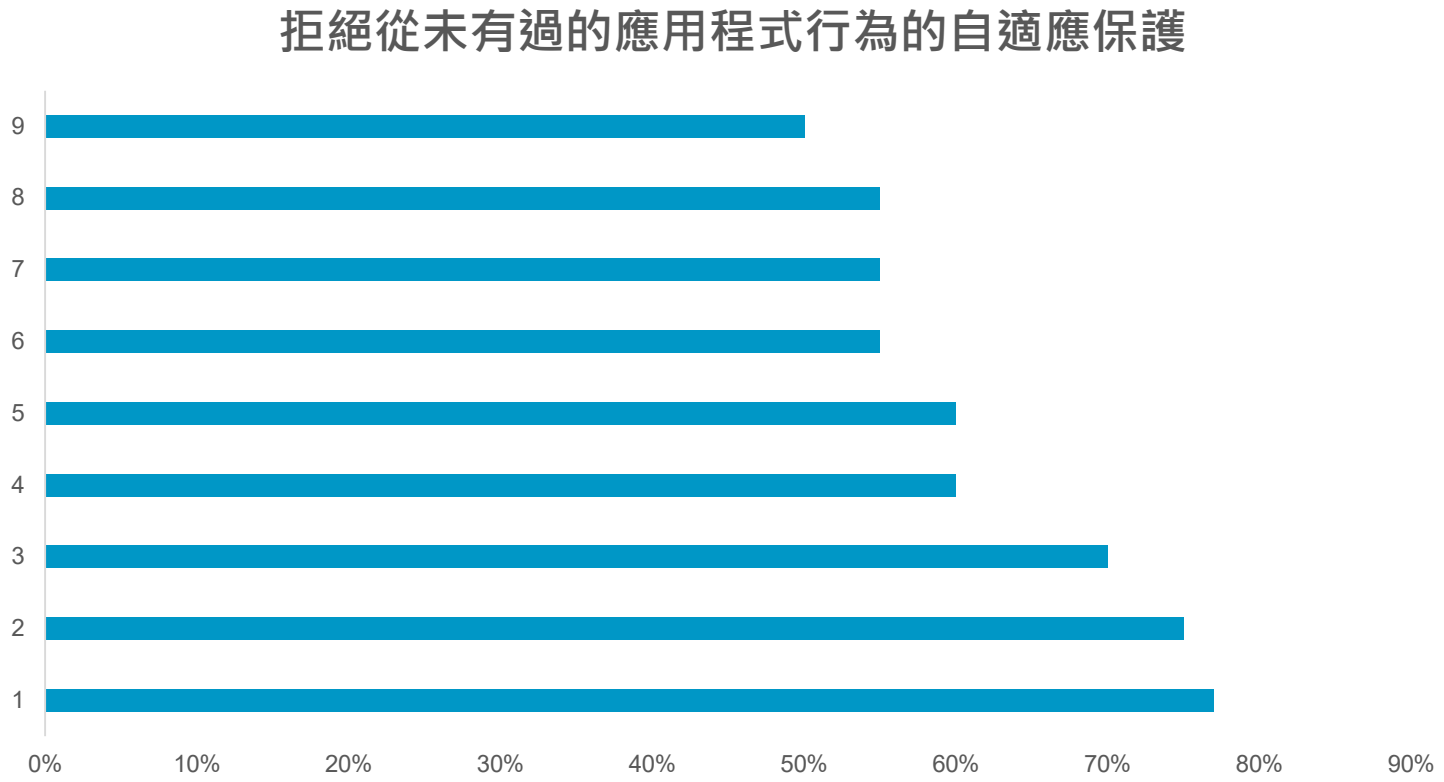

 

BROADCOM SOFTWARE

# Adaptive Protection |首日就能感受價值

## 行為改為拒絕，平均60% 第一天完全不受影響

- 自適應保護熱圖以洞察歷史資料為基礎（過去90天）填滿
- Adaptive Protection Analytics 提供客戶環境中未使用行爲的可視性
- 如果未使用行爲設置爲”拒絕”，並不會影響工作效率，但可立即減少攻擊面
- QuickTune 流程允許將所有從未有過的應用程式行為設置爲 Deny







BROADCOM SOFTWARE

# 比完整更完整的賽門鐵克端點安全完整版：SESC

- 支援所有類型端點的高級安全性
- 開放靈活的Adaptive 保護
- 偵測與回應
- 統一管理和更好的整合

BROADCOM SOFTWARE

# 主要整合

# 威脅情報 API

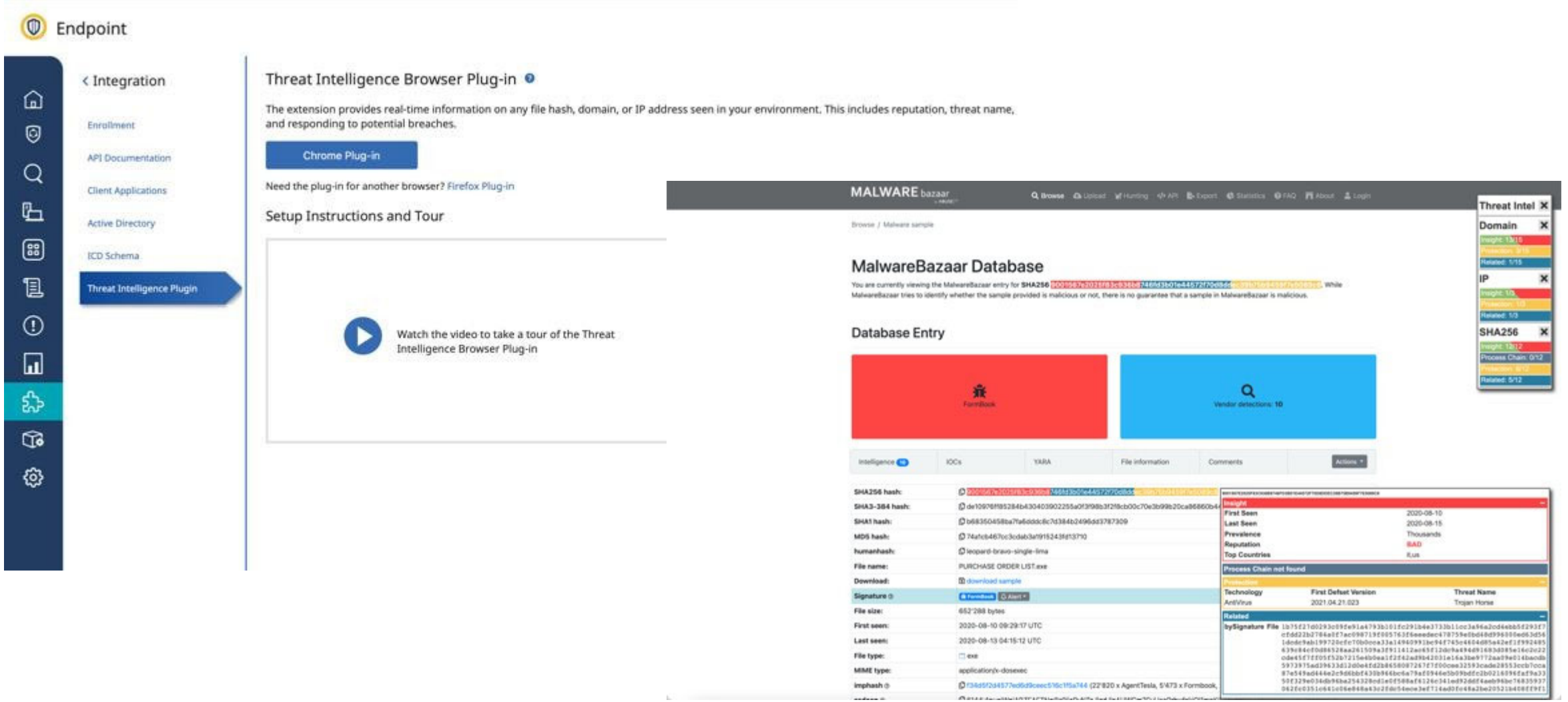
- 任何檔案的 hash、網域或 IP 位址的即時資訊包括：
  - 信譽
  - 威脅名稱
  - 普遍性
  - 壽命
  - 產業別
  - 地理位置
  - 程序歷程
  - 相關事件
    - 其他檔案
    - URLs


```
{
    "insight": {
        "targetOrgs": {
            "topCountries": [
                "us",
                "tw",
                "es",
                "de",
                "mx"
            ],
            "topIndustries": [
                "government", "information
                technology", "professional
                services"
            ]
        },
        "firstSeen": "2020-09-11",
        "reputation": "BAD",
        "prevalence": "Thousands",
        "fileSha256":
"af730c7947f9aa7bf0d6e2940b7b41774c69bacaa41cf2e5d65f
e11aca0c732a",
        "lastSeen": "2020-09-11"
    }
}
```

BROADCOM SOFTWARE

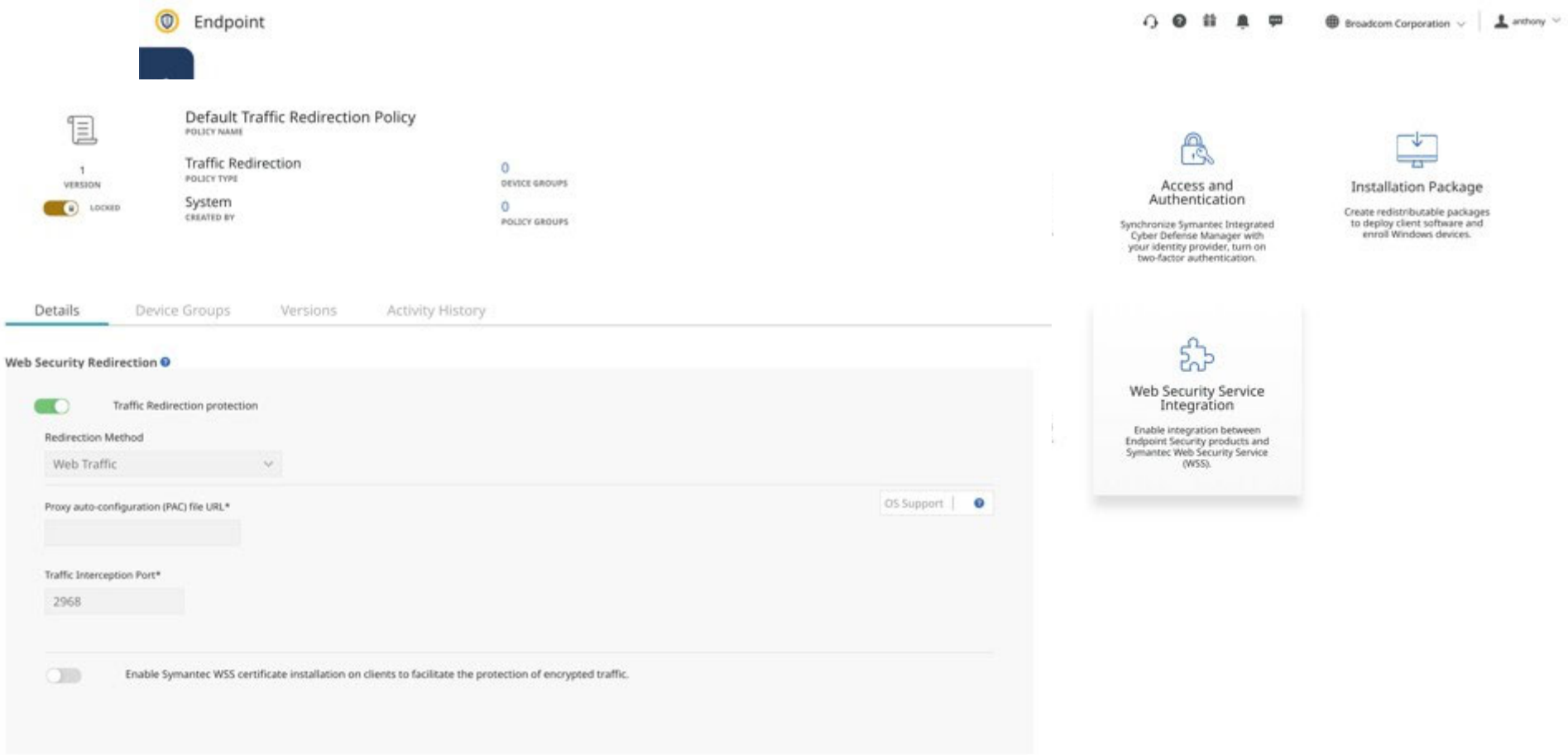
# 瀏覽器外掛



BROADCOM SOFTWARE

# 流量重導向



BROADCOM SOFTWARE

# Thank you

BROADCOM®
SOFTWARE