

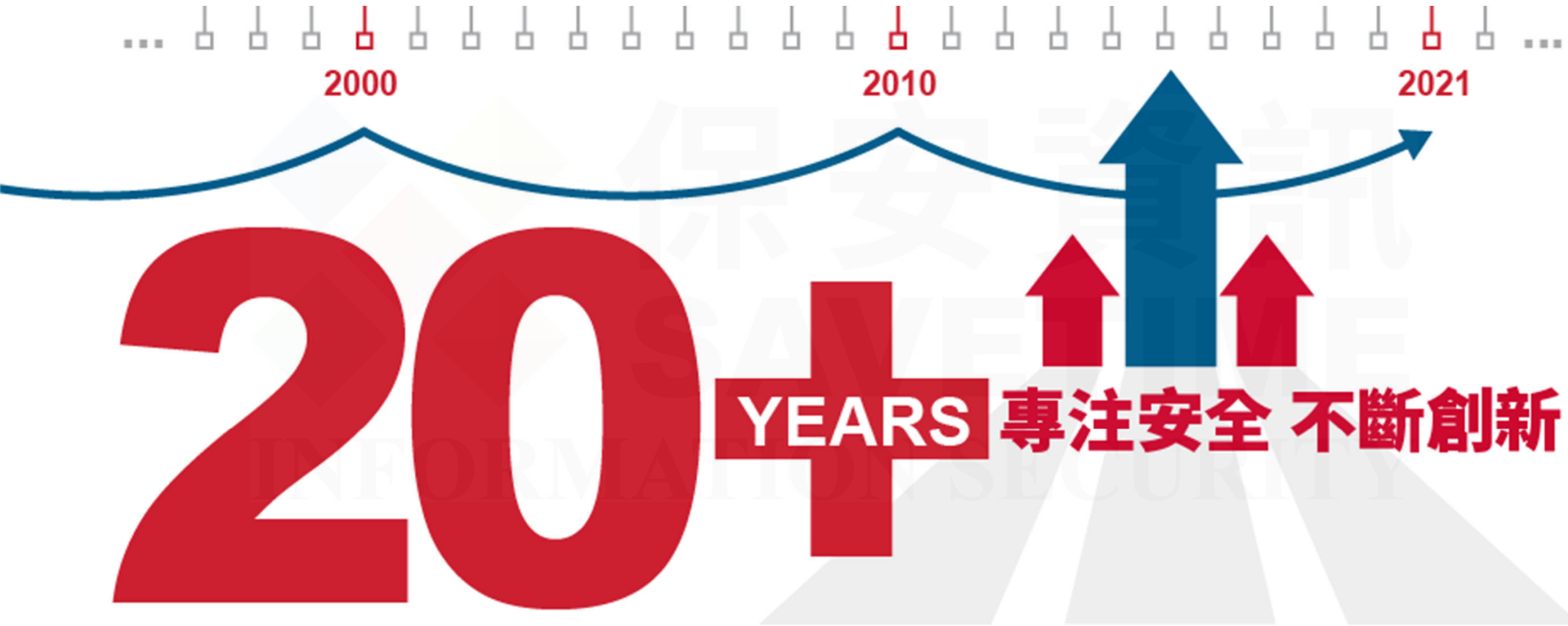

賽門鐵克全球情資網路：
隱身在賽門鐵克資安解決方案背後的強大力量

Henk Van Achterberg
產品經理 威脅情資主持人

賽門鐵克專家團隊
Bret Jordan 網路情資
Dylan Morss 雲端&App情資
Aryiro Toan 端點情資

BROADCOM SOFTWARE

賽門鐵克擁有全世界最大的資安威脅情資覆蓋範圍



Symantec
Division of Broadcom

BROADCOM

賽門鐵克全球情資網路助長卓越所有賽門鐵克解決方案

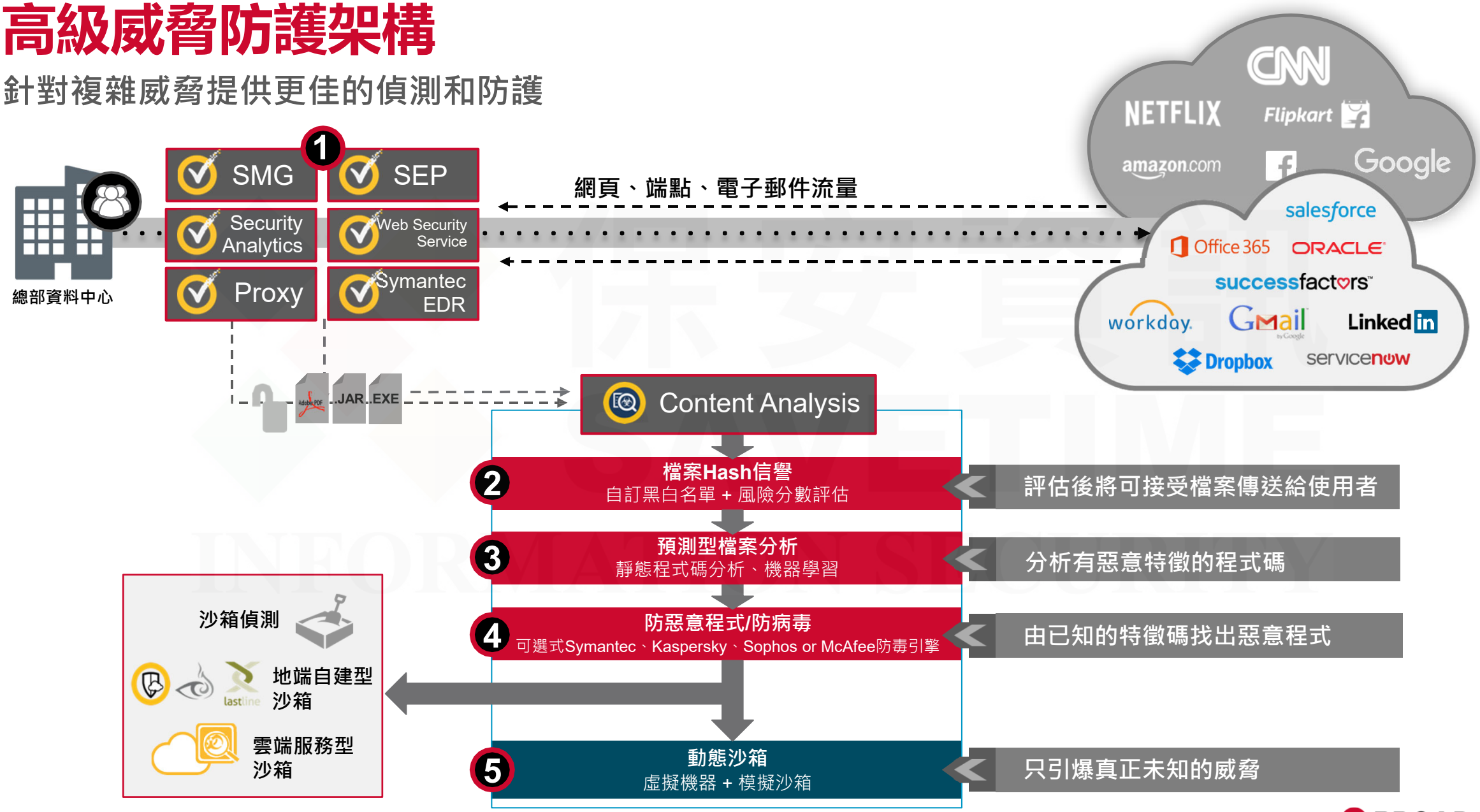
大量且全面的網路情資

- 175M(百萬)受保護的端點
- 80M(百萬)安全網頁閘道的用戶
- 160M(百萬)郵件安全的用戶
- 15,000+ 跨國大型企業用戶
- 80%財富500大的用戶
- 每天處理60種語系的10B(10億)安全回應
- 每天攔截威脅次數達數十億
- 每天分類新的網頁達數百萬篇
- 已經分類超過35,000 個雲端應用APP
- 運用超過200種不同的分析引擎

BROADCOM

高級威脅防護架構

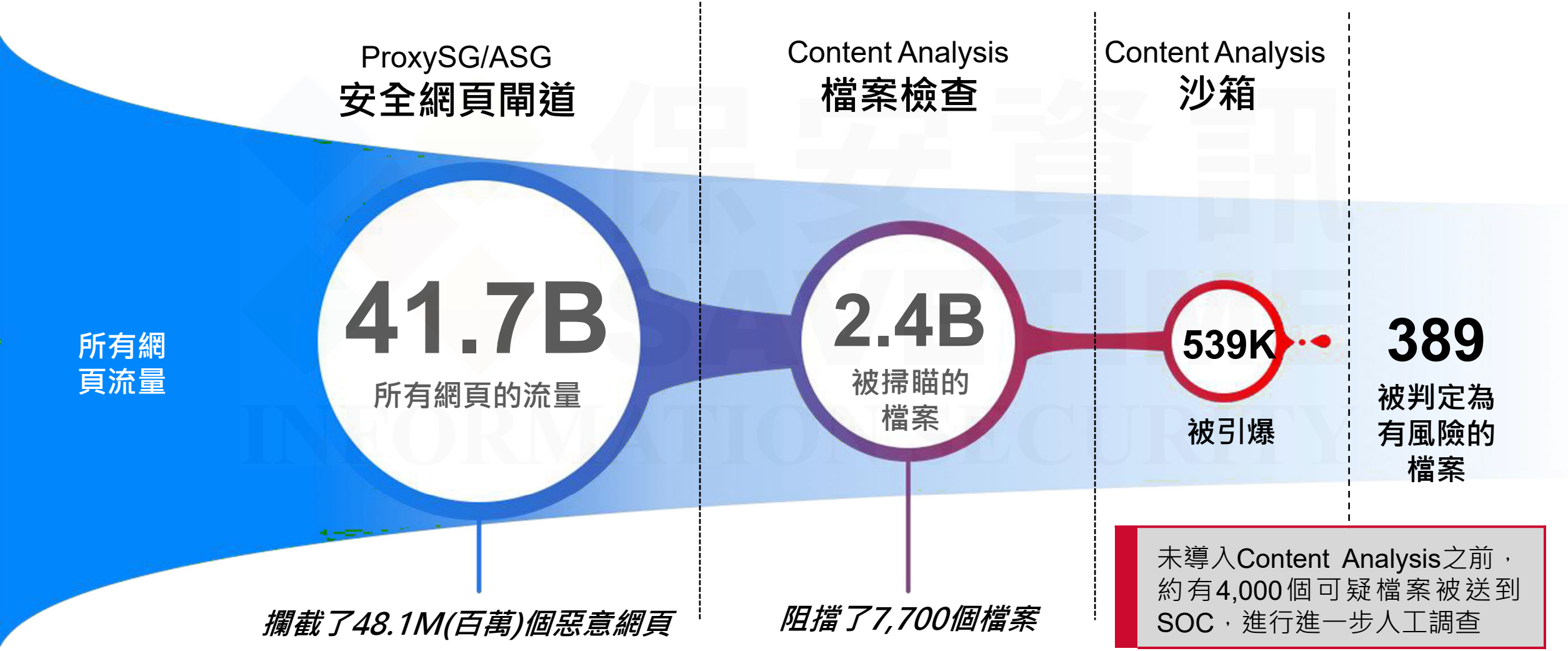
針對複雜威脅提供更佳的偵測和防護



BROADCOM

威力強大的結果：降低90%的高階人力

以某財富20大公司為實例



未導入Content Analysis之前，約有4,000個可疑檔案被送到SOC，進行進一步人工調查

*某財富20大的企業30天內的實際網路運行結果

BROADCOM

安全創新技術完整涵蓋整個MITRE ATT&CK攻擊鏈框架，保護您的環境：入侵、感染、侵擾、外滲、矯正和提升應變能力

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壞或獲，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

安全創新技術完整涵蓋整個MITRE ATT&CK攻擊鏈框架，保護您的環境：入侵、感染、侵擾、外滲、矯正和提升應變能力

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
		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			入侵預防	
		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壞或獲，停用或破獲安全軟體或正常運行	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			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

安全創新技術完整涵蓋整個MITRE ATT&CK攻擊鏈框架，保護您的環境：入侵、感染、侵擾、外滲、矯正和提升應變能力

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
		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	竄改防護	欺敵技術				入侵預防	
		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	預防惡意程式或人為破壞或獲，停用或破獲安全軟體或正常運行	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				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

由6PB遙測大數據所驅動的保護與分析

每天以20TB 的事件/日誌速度擴增大數據

端點

雲端應用程式 APPS

資料湖泊

資料擷取與移轉

以共通資訊模型(CIM)為基礎的資料清理/正規化/關聯

存儲 (Storage)

採用Google 的GCS-具高性能/全球存取規模/高可用性/高安全性等特色

經彙整的資料湖泊 (Aggregated DL)

分析

採用高可靠性的Kafka平台，處理串流資料值

採用Hive高可靠性批次處理的方式對海量資料進行處理

採用 ElasticSearch 智慧型分散式的搜尋引擎加快搜尋速度

提供現有防護強化依據

提供作為新型態的分析

提供最為第三方的分析

BROADCOM

Symantec Endpoint Protection用戰績和數據事實來保護端點安全

快速變動的威脅態勢正在顛覆整個資安產業

入侵防護技術

900M+ 每個月攔截威脅數目

9M+ 攔截勒索攻擊次數/每個月

750M+ 攔截漏洞利用攻擊次數/每個月

3.7M+ 攔截物聯網攻擊(IOT)次數/每個月

檔案檢測技術

36M+ 偵測惡意檔案(運用超過50種先進技術)次數/每個月

12M+ 採用進階機器學習科技攔截未知型或零時差攻擊次數/每個月

3M+ 攔截利用命令列或就地取材攻擊次數/每個月

2.7M+ 整合反惡意程式碼掃描介面(AMSI)攔截次數/每個月

行為偵測技術

125M+ 攔截索威脅次數/每個月

6M+ 攔截Powershell 相關次數/每個月

200K+ 攔截貨幣挖掘程式攻擊次數/每個月

BROADCOM

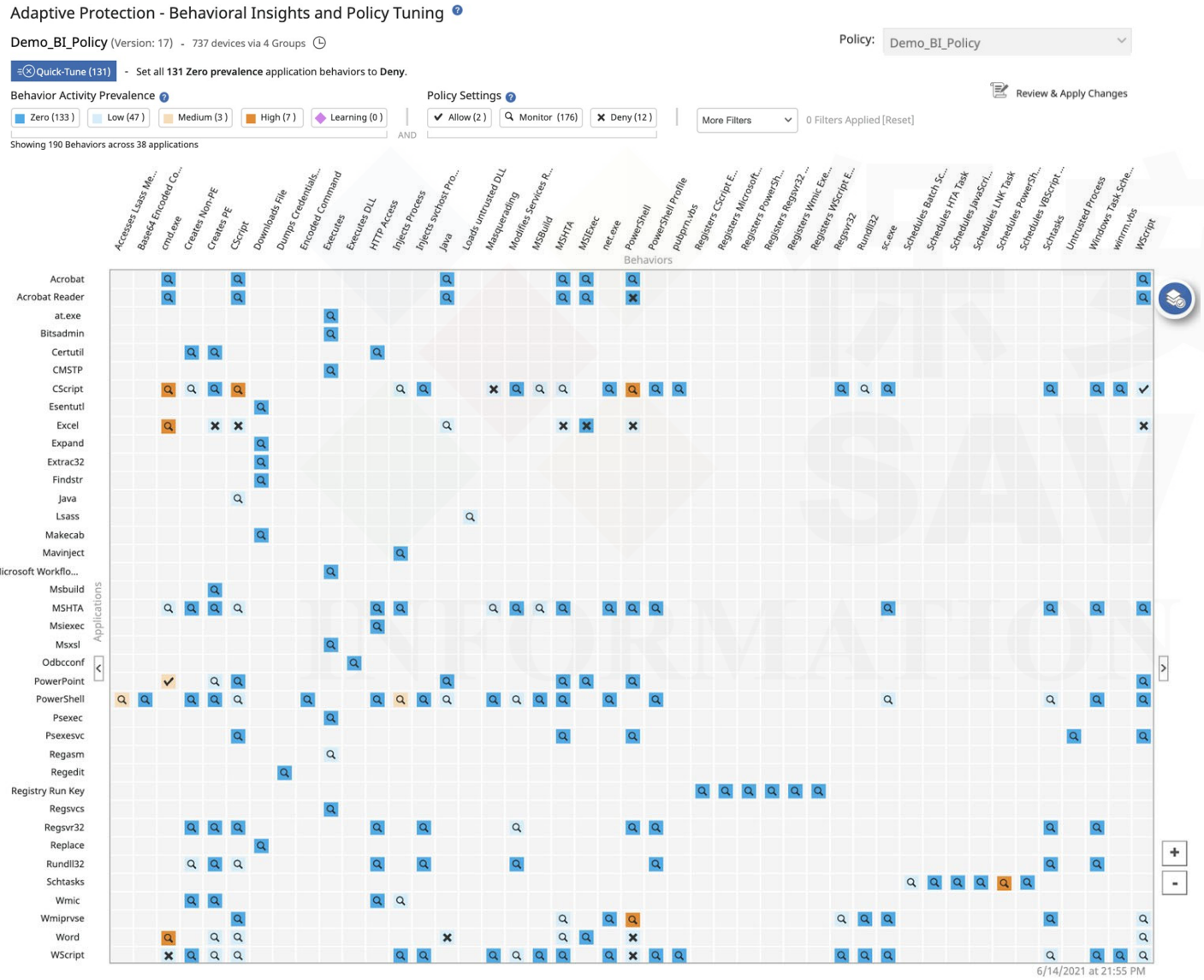
自適應(Adaptive)保護

最佳的資安防護不是「一體適用」的，反而像是DNA一樣會因人而異

- **所有顧客都是唯一的**，鐵鎚及菜刀也會因人而異成為好工具或是壞兇器
- 威脅態勢日益**複雜且更具針對性**，使用能輕易躲避安全軟體偵測的常用合法或企業專用軟體作為攻擊武器，已成為常態
- 「**一體適用**」的安全解決方案，沒有辦法提供足夠的保護力
- **攻擊者**經由不斷測試並利用發現的盲點，**可以輕易躲過**，「一體適用」的安全解決方案

BROADCOM

可調式(自適)防護 | 預防日常合法工具的攻擊



評估應用程序行為風險並提供減少攻擊面的建議。

工作原理：

- **全球遙測數據**：用於識別可信任程序的潛在風險行為
- **客戶端遙測數據**：用於識別當阻止這些危險行為的影響
- **即時**對企業中應用程式行為做**風險評估**
- 遵循**MITRE**技術分類，建議管理者相對應修正作為
- 根據企業內部危險行為的出現率提出矯正**建議**

效益：

- 監控**企業環境內自身**的程序行為
- 因應企業**不斷變化的環境和需求**，可基於風險趨勢演變進而給出最適建議
- **大大降低了攻擊成功的機會**，減少風險橫向移動的可能性

BROADCOM

您也正從全球情資網路(GIN)受益

我們提供最即時的全球情資。

只要是賽門鐵克的用戶，您可以直接利用我們開放的API獲得全球情資網路最即時的深入解析，我們內建的API，已經整合到許多主流的情資平台上，您也可以經由賽門鐵克端點安全的管理主控台來存取它。

Symantec
A Division of Broadcom

BROADCOM

威脅情資

可經由API直接存取賽門鐵克全球情資網路

即時提供威脅情資擴充

- 由**入侵指標(IOC)**的脈絡加快調查速度
- 由**關聯的入侵指標(IOC)**確認攻擊範圍
- 輕鬆與主流威脅情資平台**整合**

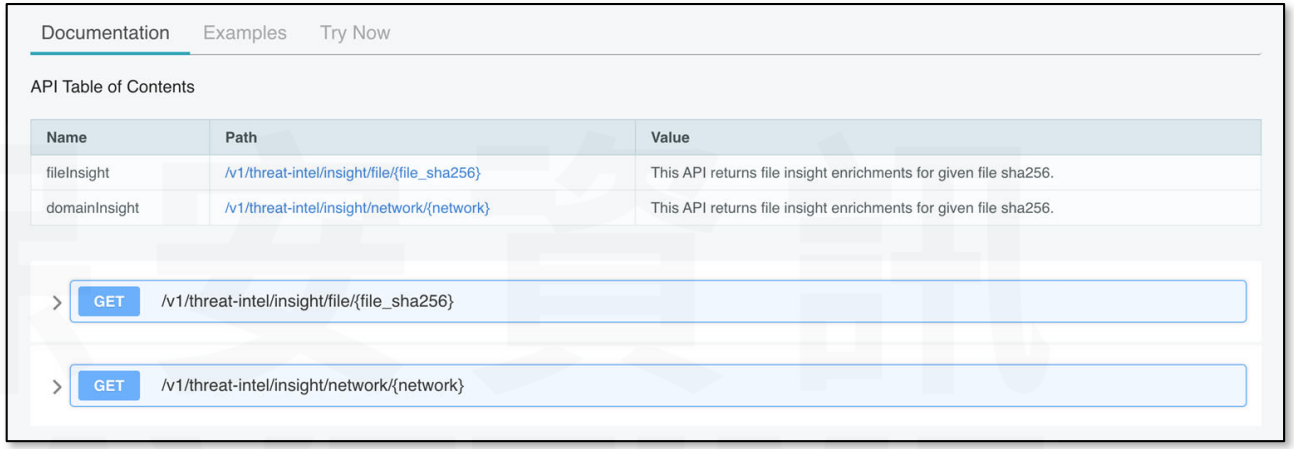
因應新興威脅與攻擊活動的戰略型資安情資

- 了解針對**特定行業或地區**的威脅或攻擊活動
- 由不斷變動的**全球威脅**態勢獲得不同的觀點以快速調整思維與應對措施
- 接獲按每天、每月、每季更新的重大威脅資訊

BROADCOM

整合選項

- **直接到 API**
  - 支援自定義工作流程
  - 立即可用
- **威脅情報平台**
  - 與其他現有的安全維運中心工作流程整合



https://apidocs.securitycloud.symantec.com

THREATQUOTIENT ANOMALI splunk> mission control

Siemplify ThreatConnect™

BROADCOM

Email Security：全面保護不斷發展的勒索軟體和其他新興威脅

1.帶有惡意程式或惡意連結的郵件

行為分析

- 深層的程式碼分析
- 檔案分解

沙箱

- 進階機器學習
- 行為與網路分析

連結保護

- 傳送電子郵件前
- 點擊時(任何時間)
- 使用進階網路釣魚變異檢測評估

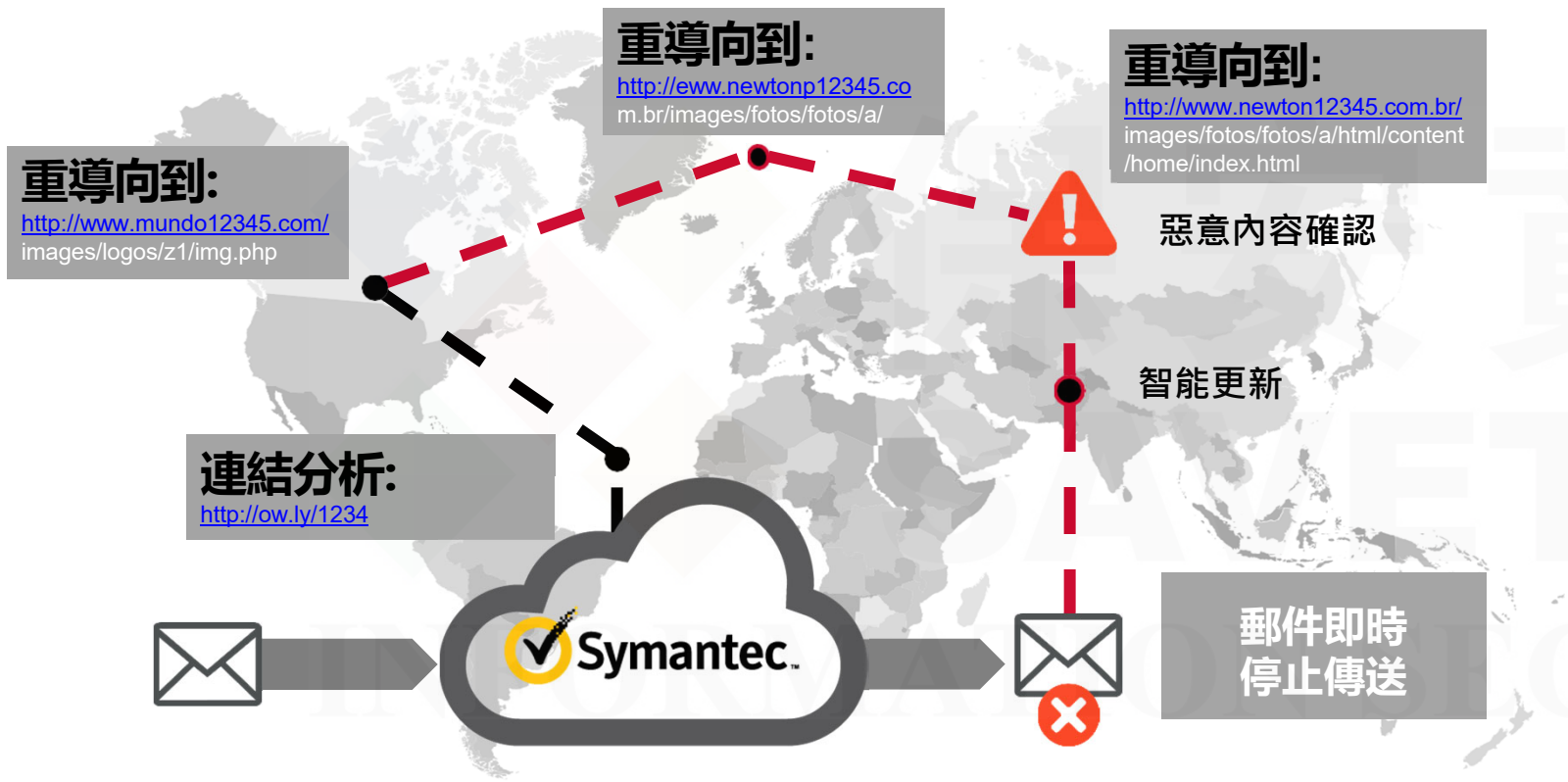
電子郵件威脅隔離

- 惡意網址(URL)隔離
- 惡意附件隔離

2.攔截惡意郵件

BROADCOM

連結追踪 - 賽門鐵克專利技術



- GIN從電子郵件遙測系統中消耗惡意軟體、網路魚和垃圾郵件URL來源
- 允許提取、掃描和追踪URL
- 判決在幾秒鐘內返回

黑名單/僅簽章方式

與Symantec Link Protection進行深度檢查

- 非依賴黑名單或簽章來評估網路釣魚連結
- 在電子郵件傳遞和點擊時評估網路釣魚連結的唯一廠商

BROADCOM

解決方案：Email Threat Isolation(郵件威脅隔離)

消除不受信任的電子郵件中網路釣魚和憑證被竊的風險

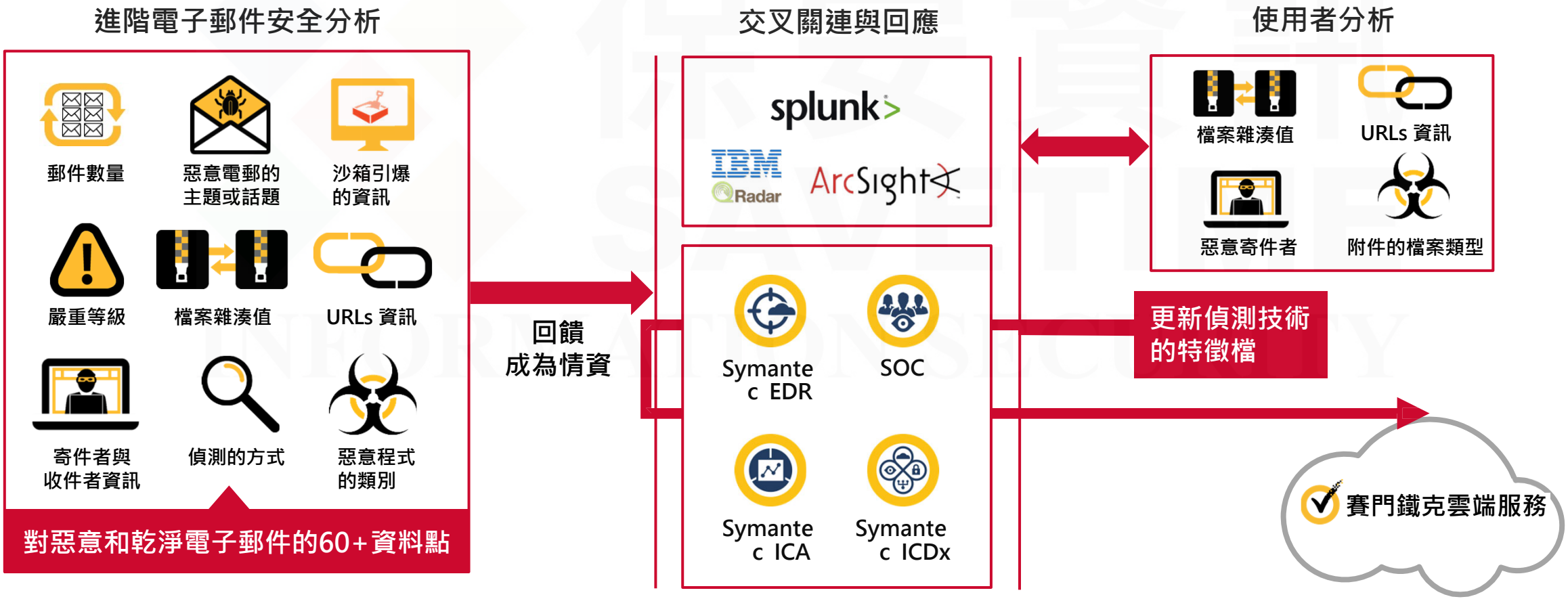
- 隔離連結和附件，以消除網路釣魚和勒索軟體的風險
- 透過在唯讀模式下渲染網路釣魚網站來防止憑證被竊
- 可在雲端或地端提供

BROADCOM

為進階威脅提供偵測與回應

根據電子郵件分析與許多常用的安全系統作關聯分析

確定目標攻擊接收者 | 可與端點威脅關聯 | 情資可分享給 web proxy | 快速找到威脅特徵 | 自動生成感染指標的黑名單 | 由威脅找出特徵



BROADCOM

情資同時整合至電郵、網路以及端點

發揮情資乘數效應

郵件安全服務(ESS)
自2018/04開始導入

內容分析(CA)
自2017/10開始導入

電子郵件：鏈結追蹤
自2018/04開始導入

進階安全閘道(ASG)
自2017/12開始導入

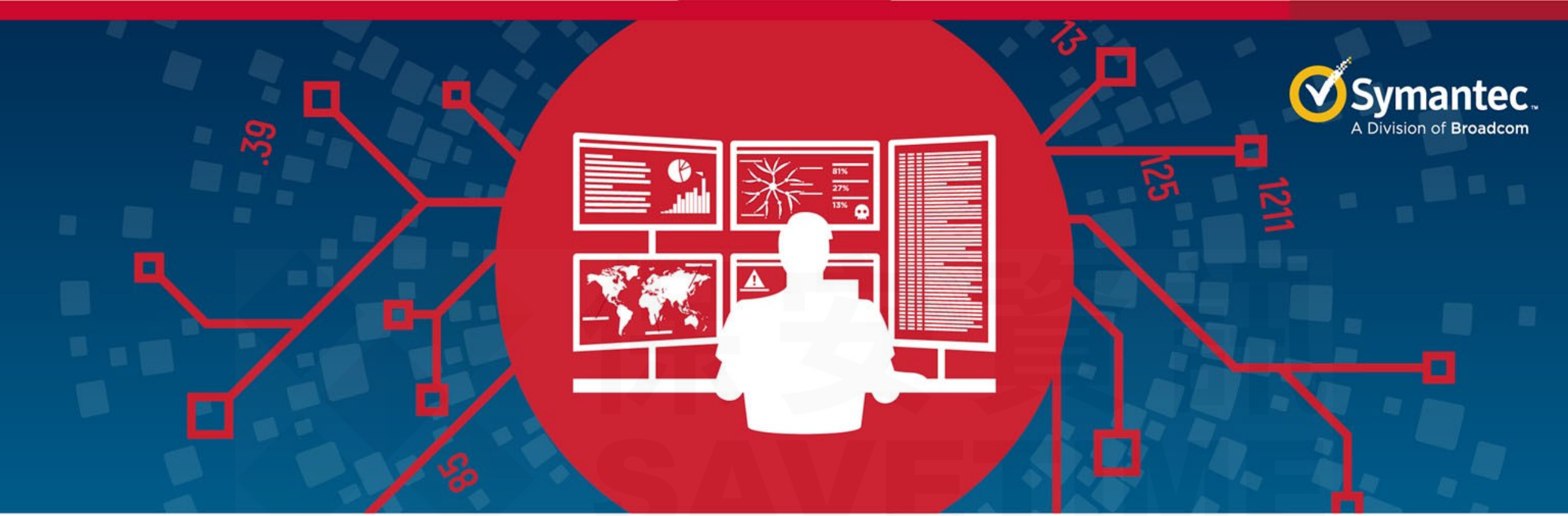
郵件安全閘道(SMG)
自2019/05/15開始導入

網頁安全服務(WSS)
自2018/02 開始導入

550萬+
最近30天所攔截的威脅數目

50萬+
最近30天所攔截的威脅數目

BROADCOM



利用安全專家的豐富經驗，發揮爐火純青的技能

我們的網路安全分析師強化了我們GIN中的洞察力，他們在全球24/7天候監控和調查威脅。他們擁有數十年的經驗，行業專業知識和深厚的技術技能——所有這些都可以讓您了解全球範圍內發生的威脅、戰術和技術的演變。

BROADCOM

不僅止於收集威脅資料

匯整分析來自四面八方、
包羅萬象的全球大數據

廣納情資，積草屯糧

包羅萬象的廣度	觀察入微的深度	鉅細靡遺的細度
175M(百萬)個端點 80M(百萬)的網頁安全代理用戶 163M(百萬)的郵件安全用戶 95M(百萬)攻擊偵測器 5M(百萬)的郵件誘捕帳號	檔案 電郵 網路 程序 系統事件	國家 產業別 實體 機器

- 收集這些事件並非易事，因為
  - 必須不能影響效能
  - 必須規避與第三方軟體產生的相衝突
  - 必須確保資料隱私的去識別化
- 基於安全前提，我們重新設計核心端點的引擎
  - 針對每個新引擎我們特別強化其在效能、隱私以及穩定性等面向的高度要求

BROADCOM

建構天羅地網、料敵如神的情資資料庫

- 建構在具有前瞻性、安全無虞且效能卓越GCP雲端基礎架構上
- 採用Hadoop、ElasticSearch、Cassandra Cassandra、Kafka...等最受歡迎的分散式大數據處理平台元件
- 情資資料庫擁有高達6PB 的大數據
  - 以每天20TB(壓縮後)的速度增加大數據
  - 擁有7TB個具有 元資料（Metadata）的檔案
  - 擁有46B(10億)個具有 元資料（Metadata）的檔案
  - 500M(百萬)程序的行為內容概況(Profiles)
  - 22M(百萬)行動的行為內容概況(Profiles)
  - 擁有2B(10億)個可疑惡意檔案
- 快速而高效搜尋能力，不到一秒鐘即能搜尋10,000筆關聯指標。

9兆列

120K
每秒回應的安全事件

BROADCOM

SESC完整版新增的威脅獵手功能

機器學習與專家分析合而為一的力量，讓潛在資安威脅的判定如虎添翼

可以發現目標攻擊活動

經驗豐富的SOC威脅獵人利用豐富的遙測和基於機器學習的雲端大數據分析來尋找和發現高準確度可疑事故。

分析團隊判別並分享相關指標

賽門鐵克威脅專家分析師發現並識別對手所使用的工具、策略、技術(TTPs)等攻擊戰術流程，並在SESC完整版的全方位功能中提供詳細的調查結果。在用戶環境中使用動態敵情跟蹤機制能監視超過150多個進階威脅攻擊組織所發動的入侵指標(IOC)。

可以存取完整的全球情資

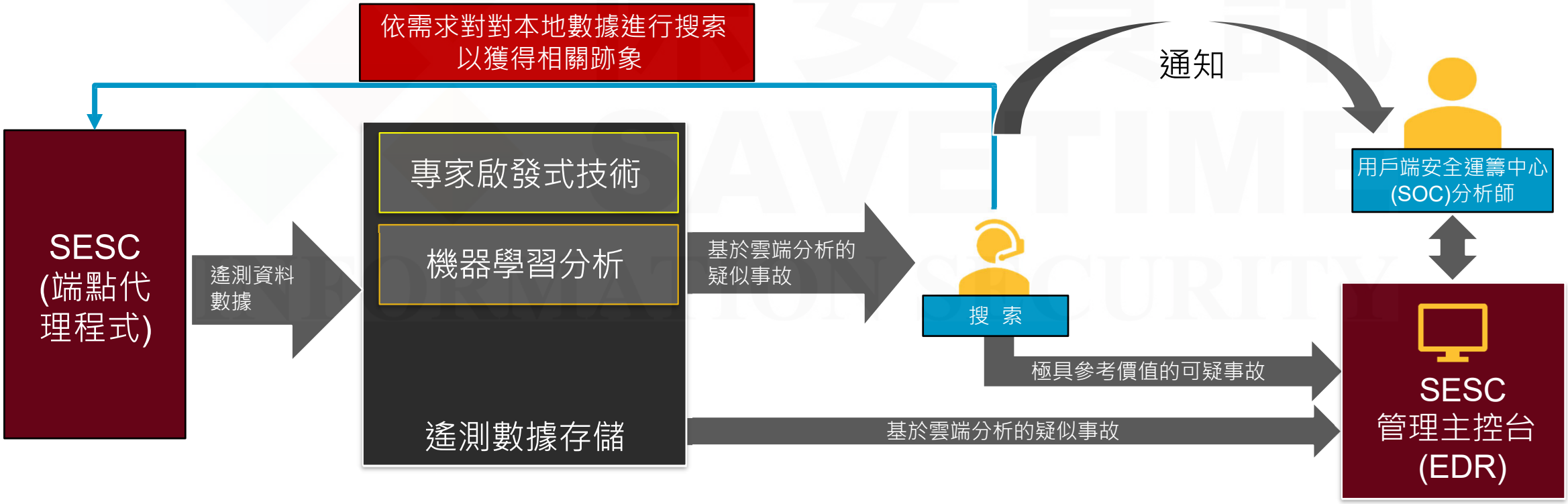
直覺式存取賽門鐵克全球安全數據的（也可透過內建的API），增強您發現和識別攻擊的能力。

第一時間就能警示通報：不管是明目張膽地公開犯罪還是鬼鬼祟祟的匿跡隱形

BROADCOM

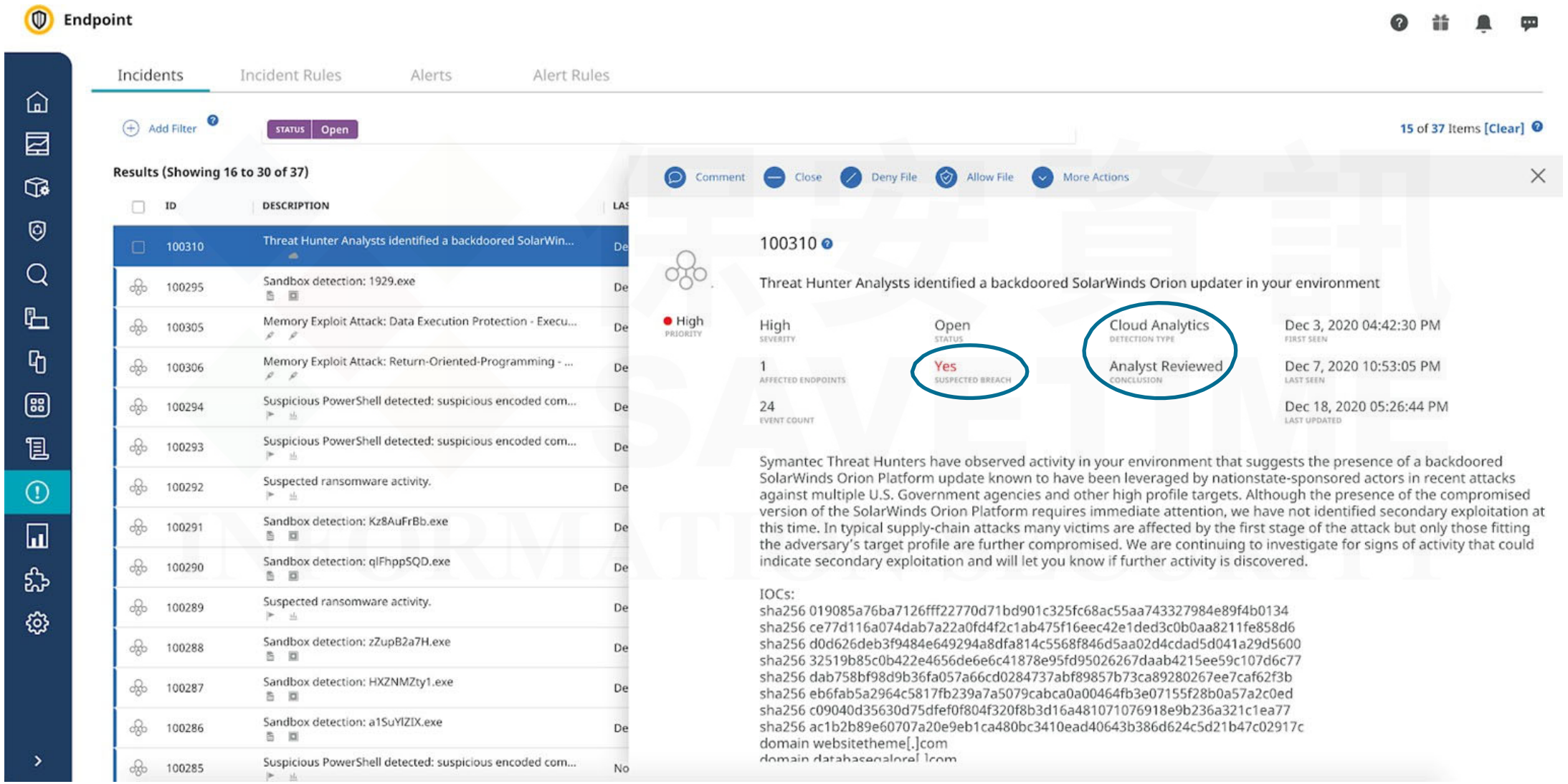
威脅獵手由世界各地眾多分析專家運用人工智慧所組成的專業團隊所支持

1. 在主控台即能透過機器學習模型及專家啟發技術產出雲端分析的可疑事故
2. 威脅獵手分析專家團隊審查並為可疑事故提供更多詳細的細節
3. 分析專家團隊主動搜索威脅並在主控台為嚴重的攻擊建立可疑事故



BROADCOM

威脅獵手 |賽門鐵克人工智慧(AI)+安全專家團隊當你的資安運籌中心(SOC)的後盾



BROADCOM

感謝您

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

保安資訊 SAVETIME INFORMATION SECURITY

相關參考資訊下載(PDF)--保安資訊整理提供

- 賽門鐵克全球情資(GIN)資訊圖表
- 賽門鐵克端點安全解決方案全覽
- 賽門鐵克郵件安全解決方案全覽
- 賽門鐵克網頁/雲端安全解決方案全覽
- 賽門鐵克端點安全在2020 MITER Engenuity ATT&CK®評比中大放異彩

BROADCOM®


BROADCOM®
connecting everything®