資安治理藍圖實踐：
打造強健的資安體質與應對策略

新加坡商威實康科技台灣分公司
首席資安顧問 曹家通 Albert Tsao

2024 May, 14

前言

ISO/IEC 27001:2022版 2013版 關鍵差異

- **2013版包含114項控制措施** 分為14章節
- **2022版包含93項控制措施** 分為4個章節

組織 37個控制措施 | **物理** 14個控制措施
人 8個控制措施 | **技術** 34個控制措施

5.7 威脅情報
5.23 使用雲服務的信息安全
5.30 ICT為業務連續性做好準備
7.4 物理安全監控
8.9 配置管理

控制措施差異

- **沒有刪除任何控制措施** 但許多項合併一起, 從而減少了總數
- **2022版引入11個新控制措施**

8.10 信息刪除
8.11 數據屏蔽
8.12 數據洩露預防
8.16 監控活動
8.23 網頁過濾
8.28 安全編碼

轉版時程

2022/10 2022新版發布

2024/5/1 新申請不可再使用ISO/IEC 27001:2013版本稽核

2025/10/31 ISO/IEC 27001:2013 **舊版證書失效**

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- ## 5.7 威脅情報

應蒐集並分析與資訊安全威脅相關之資訊,以產生威情資。

※ 可用產品類型說明：

如: 威脅情報平台可收集、分析和分享關於最新威脅和攻擊的資訊，協助組織即時掌握威脅情勢，並採取適當的防禦措施。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

Symantec Global Intelligence Network

Sees What Others Cannot

HUMAN EXPERTISE

Threat Hunters monitor 24/7, issue alerts, create protection and publish Threat Intel

- 50+ ransomware families tracked
- Recent discoveries included
  - ShuckWorm
  - Daxin
  - BumbleBee

TECHNOLOGIES

50+ protection technologies focused on prevention, not detection.

- AI/ML
- Exploitation, not Threat Detection
- Behavior Blocking
- Adaptive Hardening

ANALYZED DATA

9 Petabytes and Growing

- 2B suspicious files
- 6B Digital signatures
- 22M mobile profiles
- 46B URLs
- 500M process behaviors

Results:

(September 2022)

1M+
Ransomware
Attacks Blocked

1.5M+
Living-off-the-land
Threats Blocked

2.7M+
Unknown and 0-day
Attacks Blocked

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- **7.4 物理安全監控**

  應持續監視場所,防止未經授權之實體進出。

  ※ 可用產品類型說明：

  如: 系統可以通過監視攝像頭、入侵檢測器等技術，實時監控組織內部和外部的物理安全狀態，並及時警報和記錄可能的安全事件。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- **8.9 配置管理**

  應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)

※ 可用產品類型說明：

如: 這類工具可幫助組織管理和控制IT系統和設備的配置，包括軟體和硬體配置，並確保它們符合安全和合規要求。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- ## 8.10 信息刪除

當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時,應刪除之。

※ 可用產品類型說明：

如: 數據刪除軟體能夠徹底刪除敏感資料，包括文件、資料庫和儲存設備中的數據，以防止其被未經授權的人訪問或恢復資料。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- ## 8.12 數據洩露預防

應將資料洩露預防措施,套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。

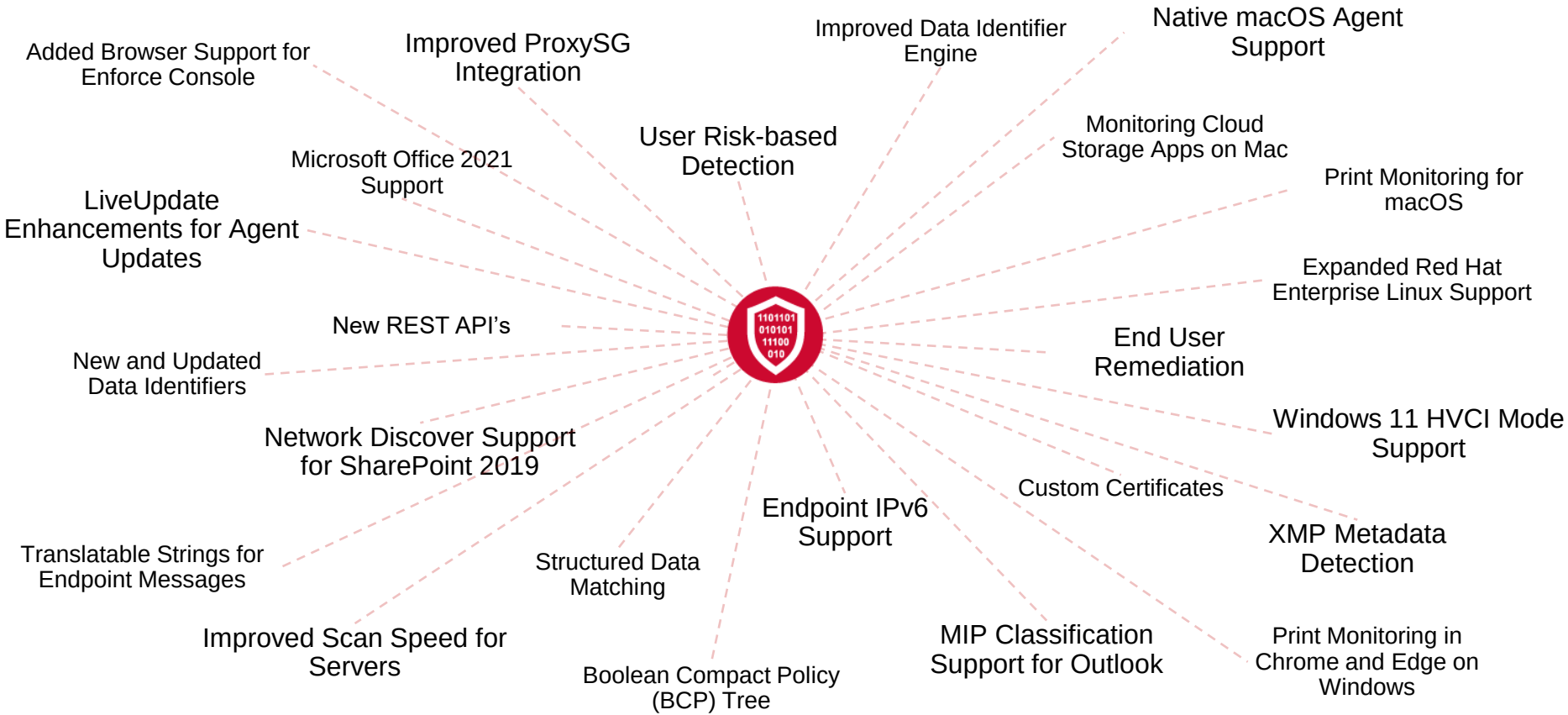
※ 可用產品類型說明：

如: 這解決方案能夠檢測和阻止敏感數據意外外洩的行為，並提供實時監控和警報功能，幫助組織及時應對潛在的風險。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

Recent DLP Development Highlights



DLP 廣泛的涵蓋範圍

Symantec by Broadcom

DLP 90% 都是事件回應

做正確的事，減少資安事件處理所花費的時間

正確的指標 |

與高階主管及稽核部門

進行驗證

正確的自動化設定 |

定義, 執行, 通知及記錄

正確的執行 |

一鍵回應

正確的人員 |

將事件傳送給正確的管理者

正確的訊息 |

5秒的快速測試

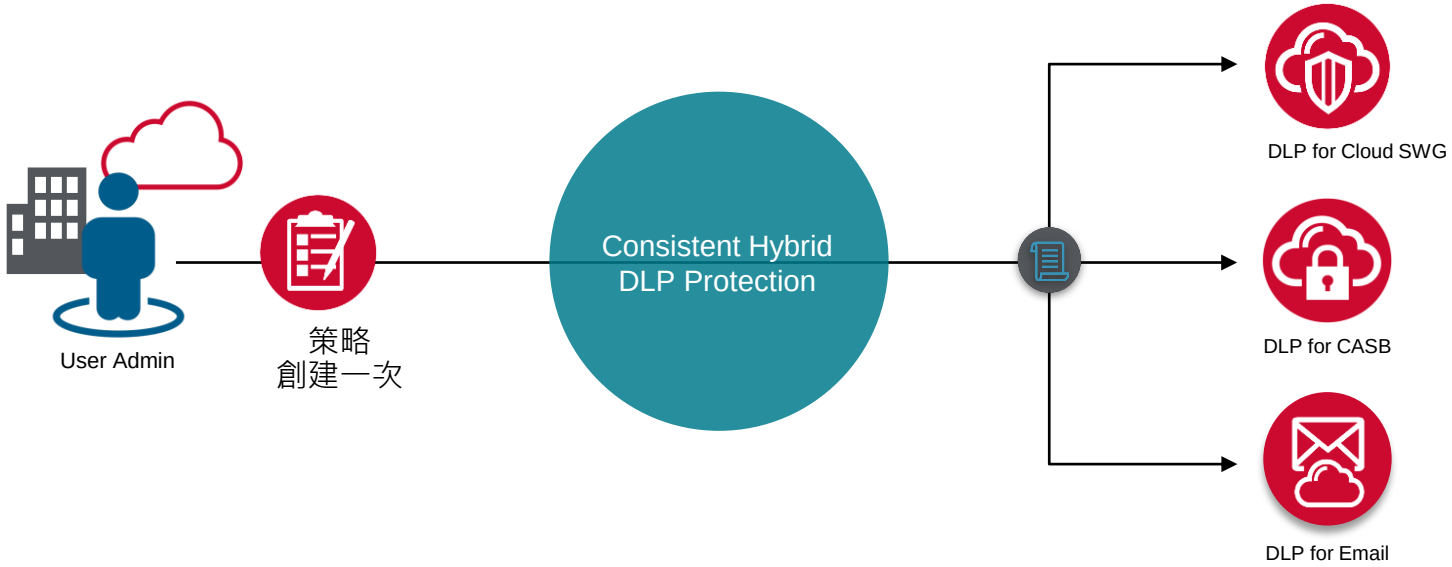
正確的順序 |

依事件嚴重及優先順序

Symantec by Broadcom

保護無所不在的數據資料

綜合政策一致適用於所有資料傳遞管道



豐富的檢測能力

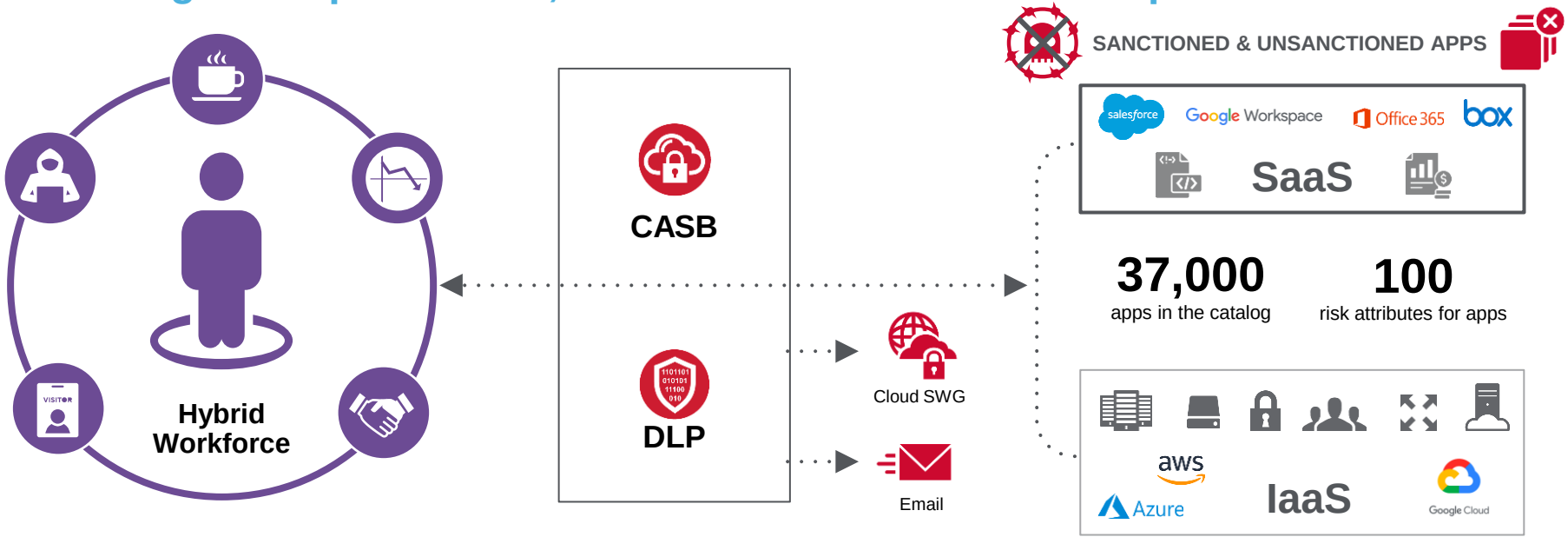
使用者分析

補救措施

Symantec by Broadcom

DLP in the Cloud

Delivering a comprehensive, secure and seamless user experience



Gain granular visibility & control in the cloud and uncover Shadow IT

Monitor and protect sensitive data at rest and in motion in apps

Identify risky behavior and defend against a host of cloud threats and malware.

Compliance Assurance in SaaS & IaaS

Continuously monitor risk and respond to security events quickly.

Symantec by Broadcom

DLP for Web

使用 Cloud/Edge SWG 保護您的數據

解密流量以提供 DLP 檢查內容

保護您的資料不外洩到目的地網路

SWG 根據 DLP 策略阻止使用者操作

透過 DLP 實現統一政策與事件管理

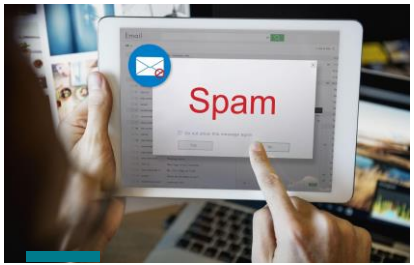
Symantec by Broadcom

DLP for Email - Office 365 and Gmail

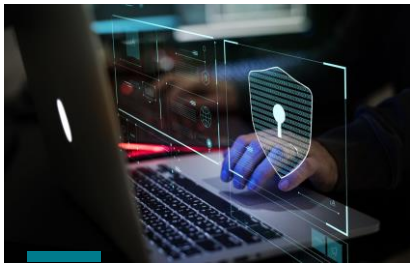
防止電子郵件中的資料遺失和針對性的攻擊

我們如何透過電子郵件保護您的資料？

電子郵件是導致資料遺失的首要媒介



根據 DLP 策略檢查電子郵件內容。

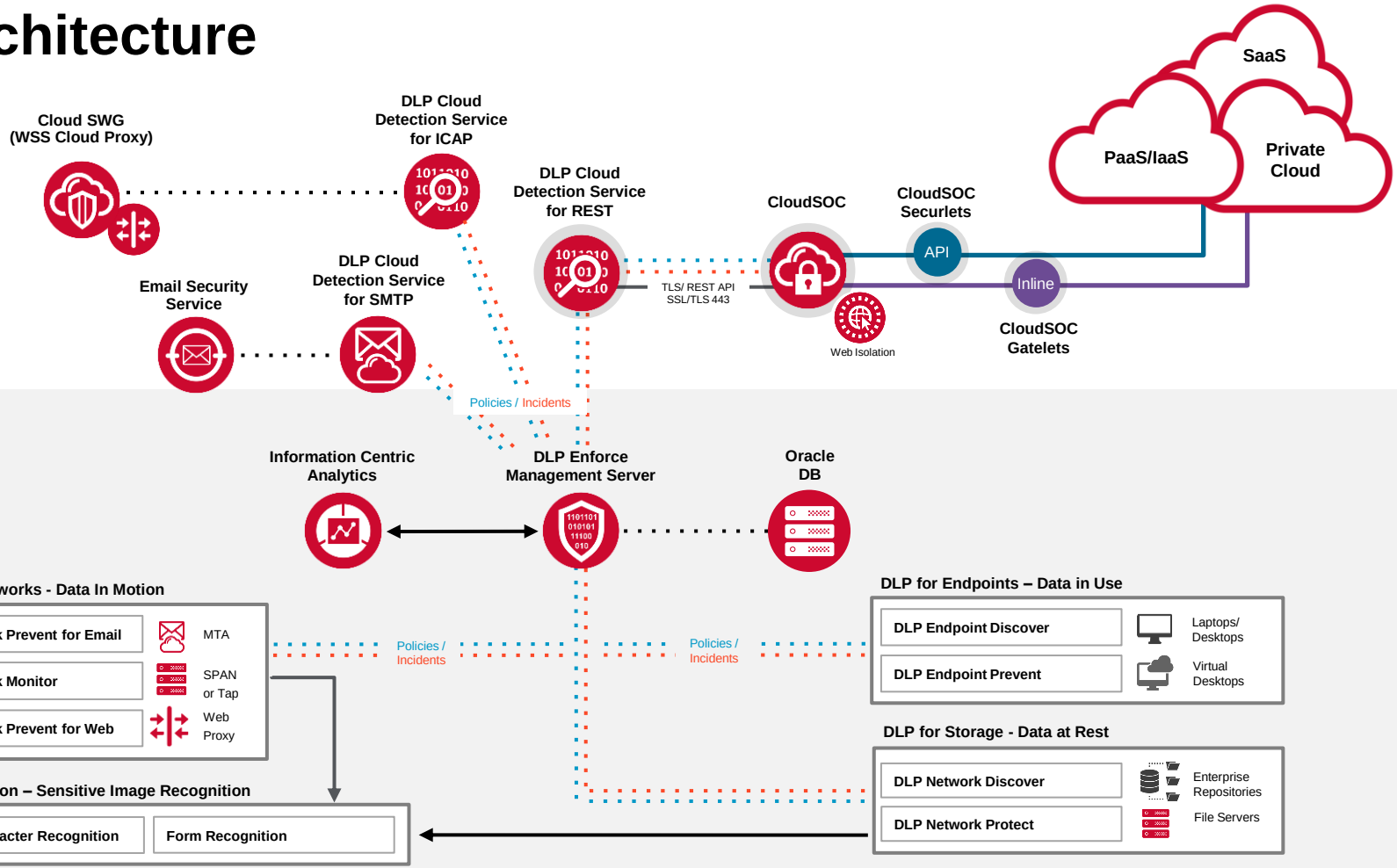


阻止/隔離電子郵件以防止機密資料洩露

透過 DLP 實現統一政策與事件管理

Symantec by Broadcom

DLP Architecture



DLP + Microsoft Information Protection (MIP)

提高可見性和保護

Crack open MIP Files

DLP 能夠在所有 DLP 控制點上檢查受 MIP 保護的文件和電子郵件

Read MIP labels

DLP 能夠在所有 DLP 控制點上讀取文件和電子郵件上的 MIP 標籤

Drive MIP labels

使用進階偵測功能在端點上建議或強制執行 MIP 標籤

Symantec by Broadcom

ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- **8.16 監控活動**

  應監視網路、系統及應用之異常行為,並採取適切措施,以評估潛在資訊安全事故。

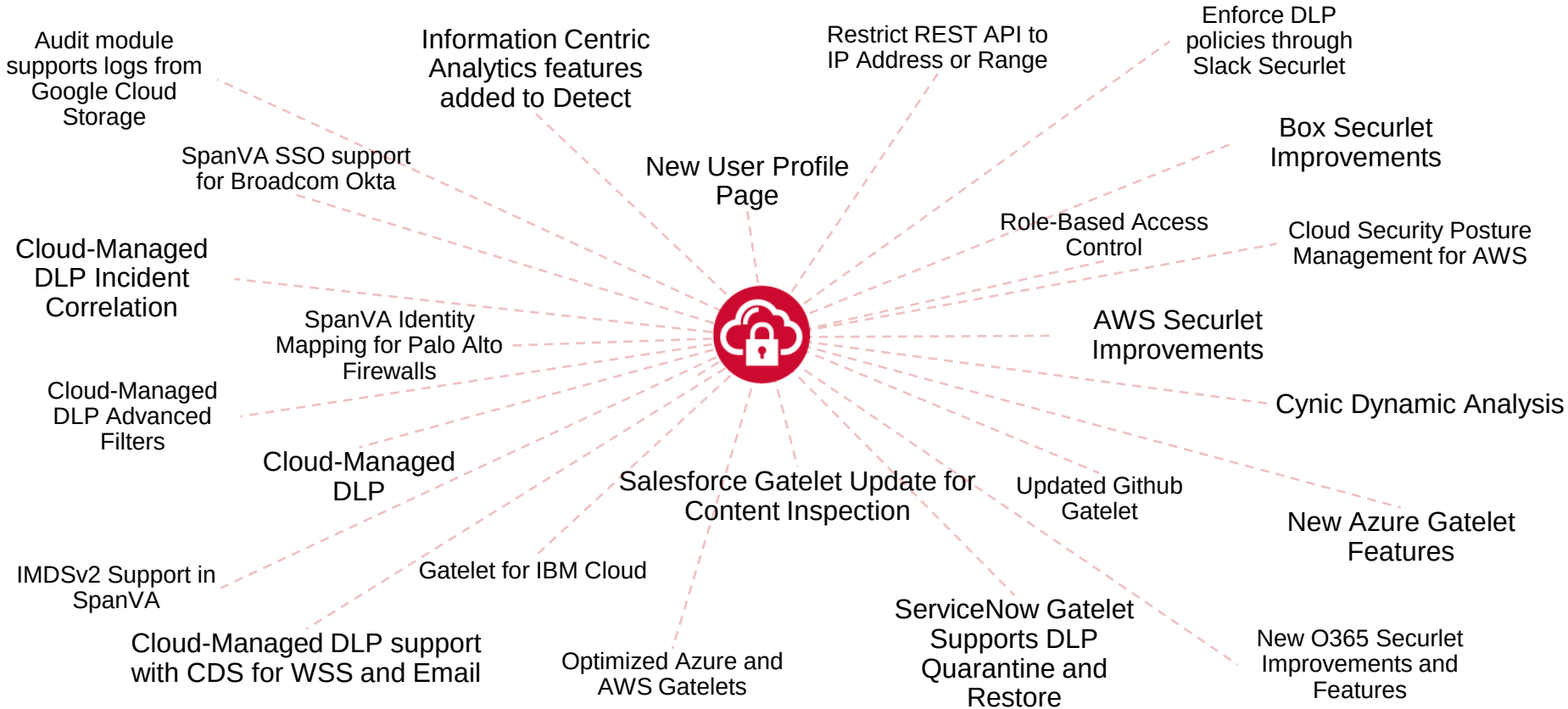
  ※ 可用產品類型說明：

  如: SIEM、SOAR、N-Cloud系統，它能夠收集、分析和識別IT環境中的安全事件和活動，並提供實時警報和報告，幫助組織迅速響應安全事件。

資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

Recent CASB Development Highlights



ISO/IEC 27001 之 2022 版與 2013 版關鍵差異

- ## 8.23 網頁過濾

  應管理對外部網站之存取,以降低暴露於惡意內容。

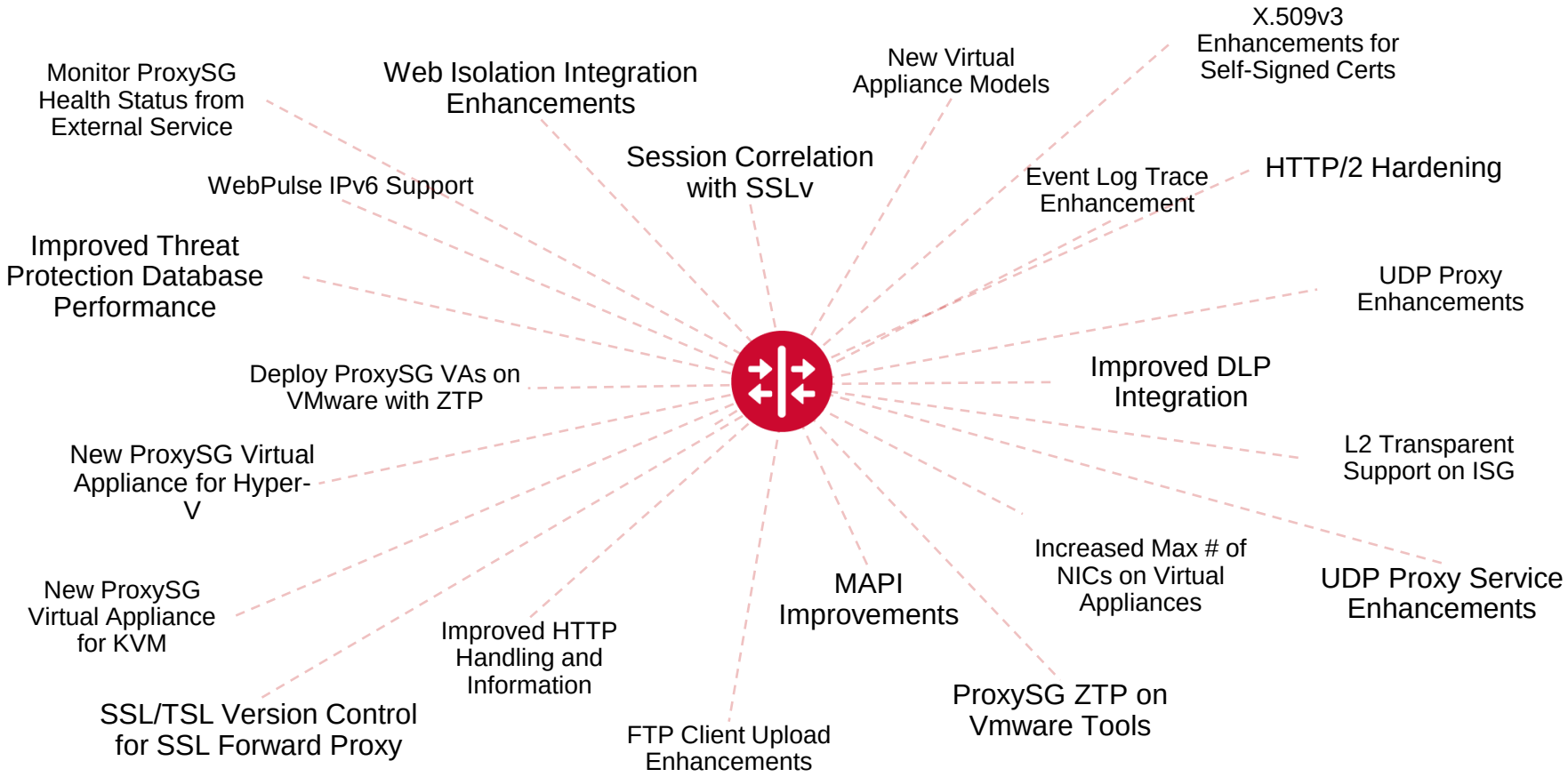
※ 可用產品類型說明：

如: 這類產品能夠檢測和阻止網路流量中的惡意網站、廣告和內容，保護用戶免受網路攻擊和不良內容的影響。

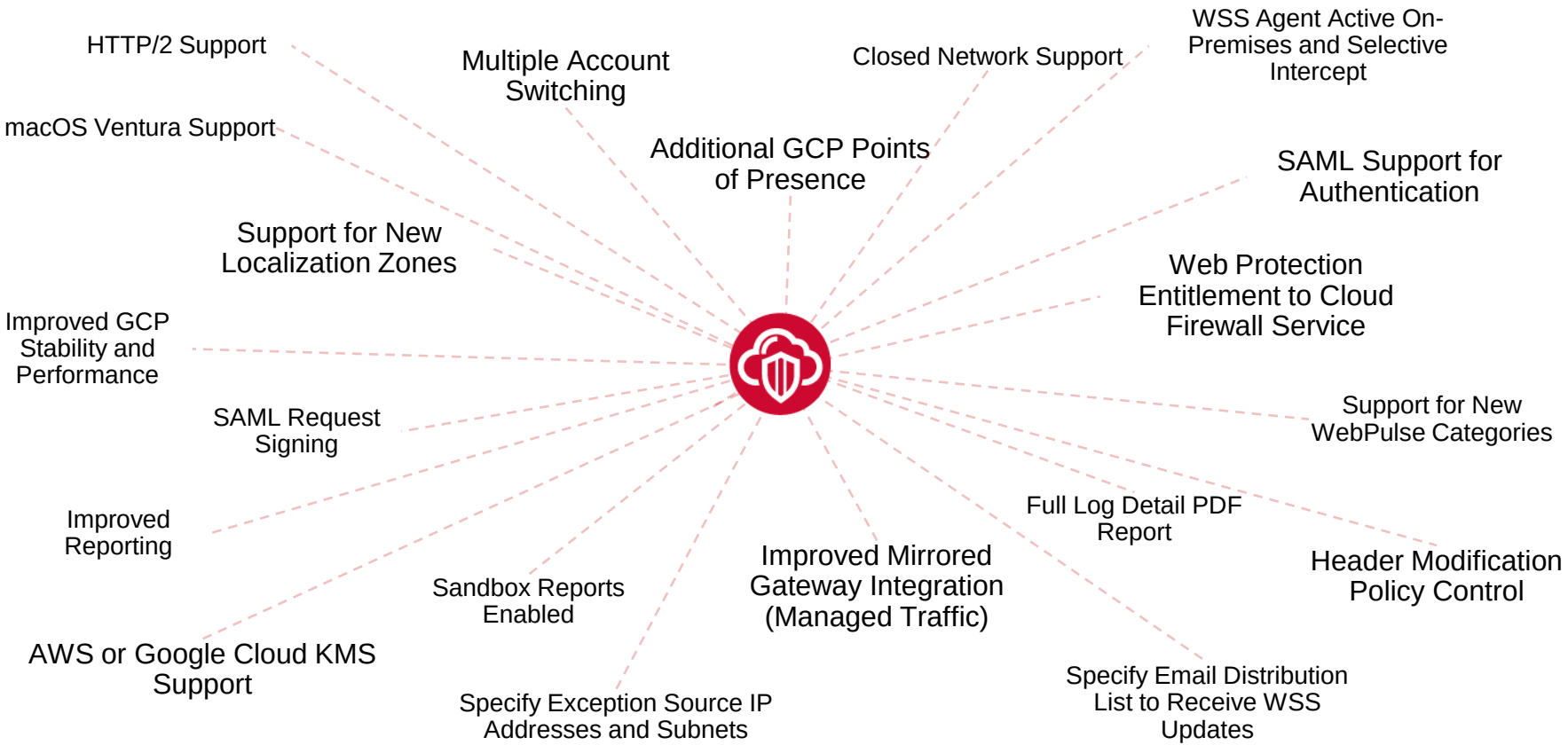
資料來源： 網安智慧科技股份有限公司 Network Security intelligence Technology Co., Ltd. 技術合作夥伴

Symantec by Broadcom

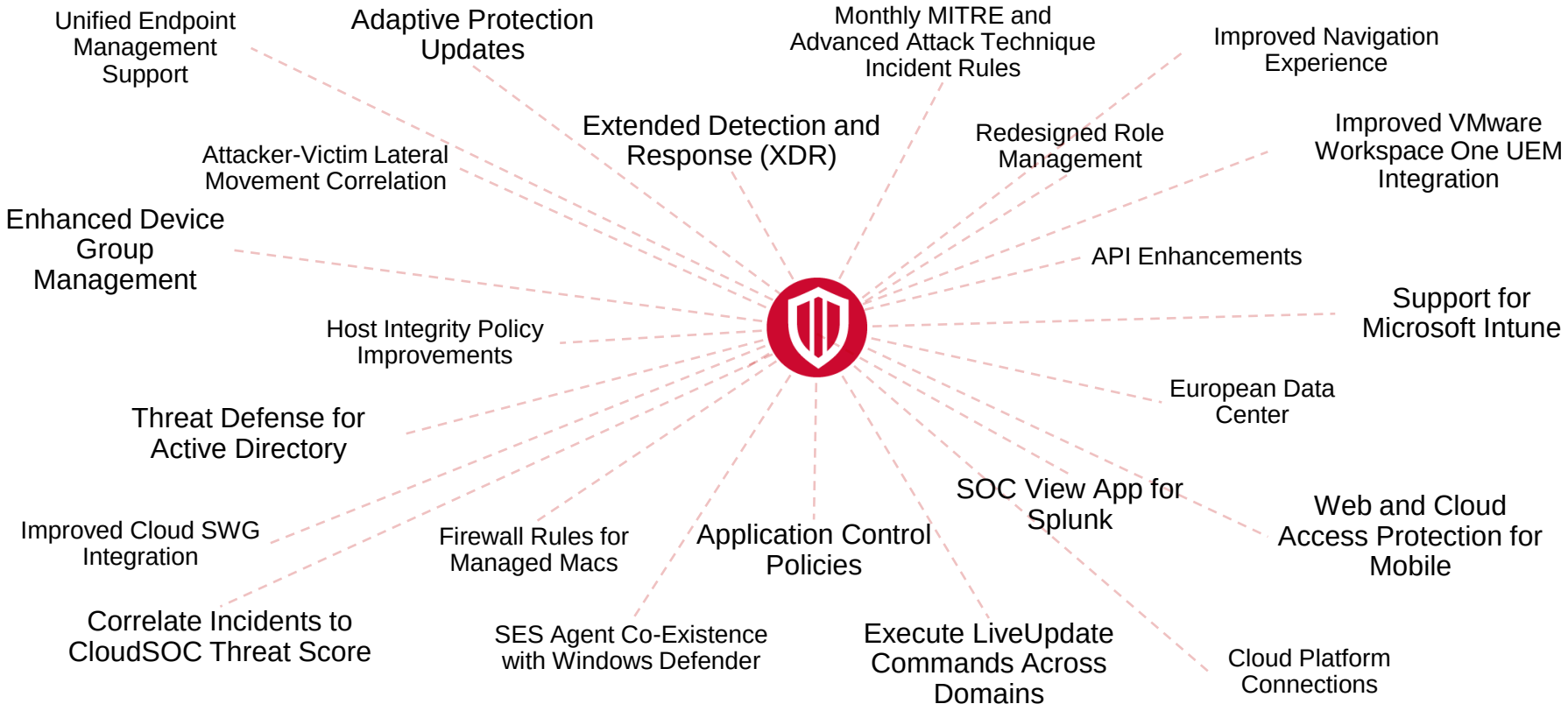
Recent Edge SWG Development Highlights



Recent Cloud SWG Development Highlights



Recent Endpoint Development Highlights



Zero Trust Network Access

支援混合安全，安全替代VPN

87% 的企業制定了混合雲策略

Flexara

96% 的 SASE 採用者也計劃採用 ZTNA

ESG Research SASE Key Trends 2022

86% 的 SASE 採用者正在積極部署 ZTNA

ESG Research SASE Key Trends 2022

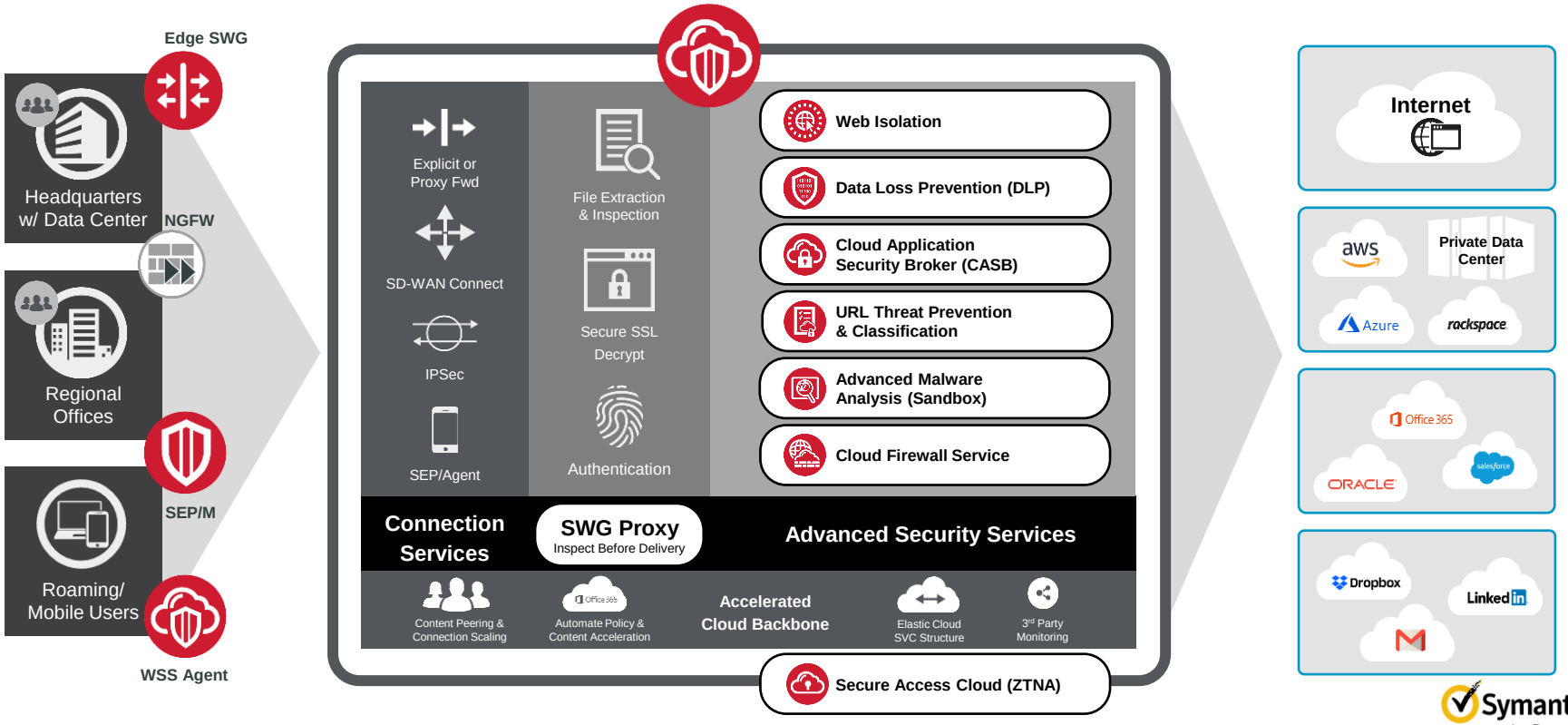
Symantec Zero Trust Network Access

點對點連線隱藏所有企業應用程式和資源，消除橫向移動和基於網路的威脅

Symantec by Broadcom

Symantec Enterprise Cloud

Network Protection is key to achieving Zero Trust



Symantec by Broadcom

Symantec Intelligence Services

Intelligence powers Network Protection

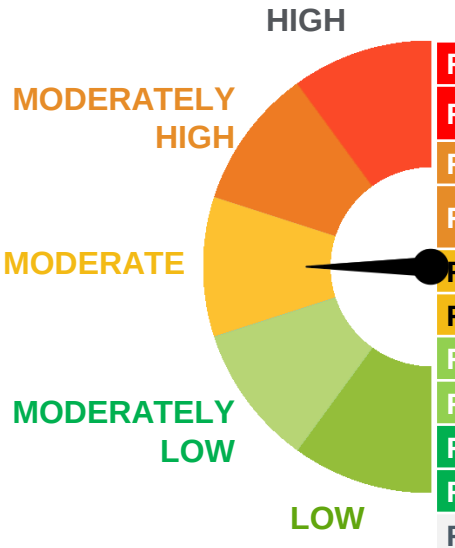
Intelligence Services

- 將Web分為 80 多個預先定義類別，其中包括 12 個安全類別
- 使用雲端中 200 多個可識別 60 多種語言的人工智慧模組對新網站和未分類網站進行即時分類
- 每個網站的威脅風險等級評級，無論是否可以分類網站的
- 地理位置訊息，可以按國家/地區位置應用政策

Symantec by Broadcom

Cloud Delivered Intelligence – Advanced Intelligence Services

Enabling granular security and acceptable use policy



Risk Level 10:	Solid evidence of malicious (rated in database)
Risk Level 9:	Probably malicious
Risk Level 8:	Stronger evidence of maliciousness
Risk Level 7:	Shady behavior (including Spam, Scam, PUS, etc. but possibly malicious)
Risk Level 6:	Exercise caution; very new sites, or some evidence of shady behavior
Risk Level 5:	May not be safe; no established history of normal behavior
Risk Level 4:	Still probably safe (or starting to establish a history of normal behavior)
Risk Level 3:	Probably Safe
Risk Level 2:	Other top sites; consistently well-behaved
Risk Level 1:	Big names; long history of good behavior; huge traffic
Risk Level 0:	Customer Allow List

Cloud Delivered Intelligence Services

Categories

Risk Levels

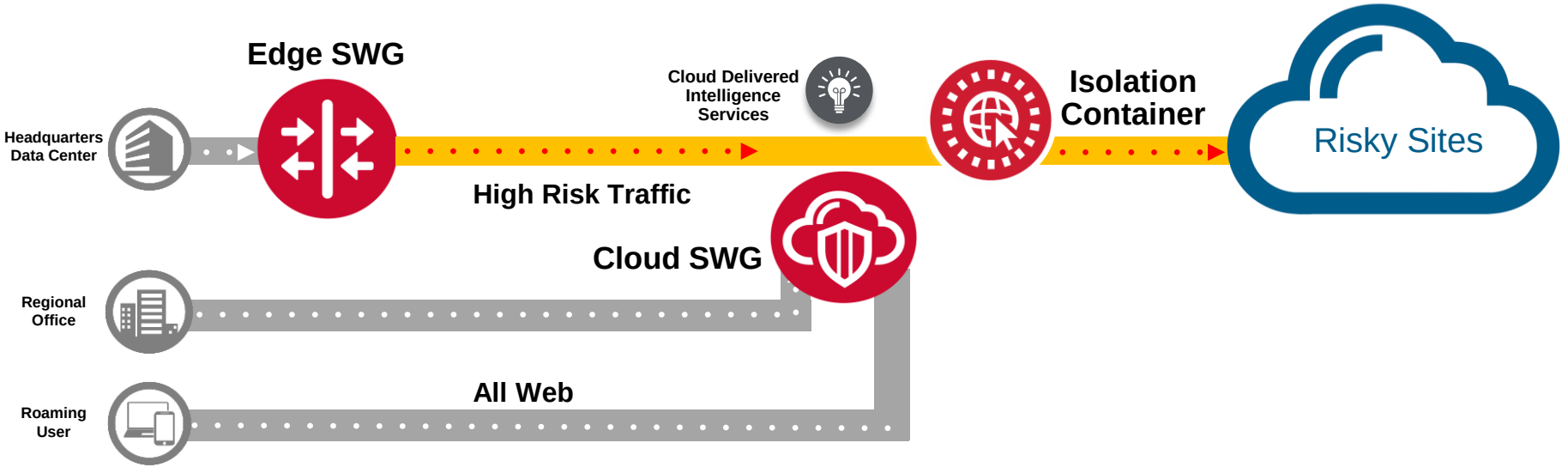
Application Visibility

GeoIP

Symantec by Broadcom

High Risk Isolation

Remote access to risky and unknown sites



Allow SecOps to focus on high-value activity vs block/allow policy

End users are productive while browsing uncategorized sites

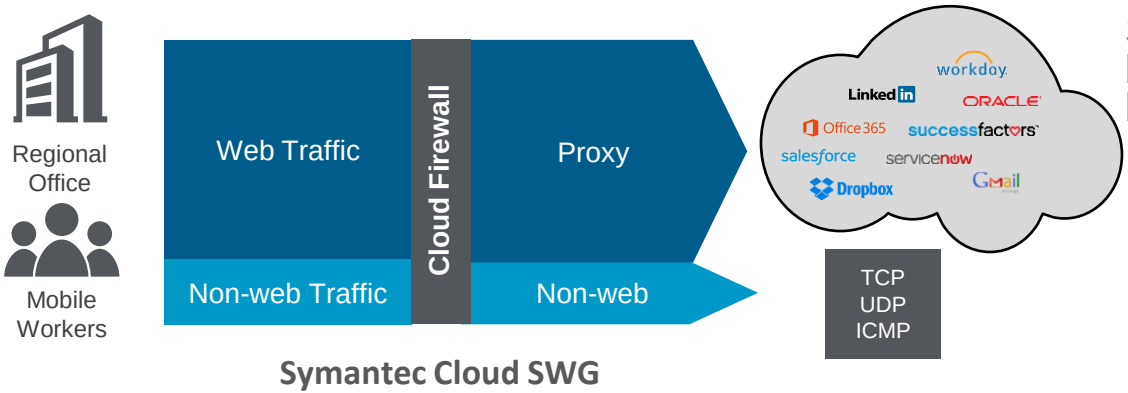
Prevent phishing and credential theft with Read-only access option

*Must have SGOS 7.3.1 or higher

Symantec by Broadcom

Symantec Cloud Firewall Service

Securing All Internet Traffic



Secure ***all internet traffic*** for internet breakouts in remote offices & branches

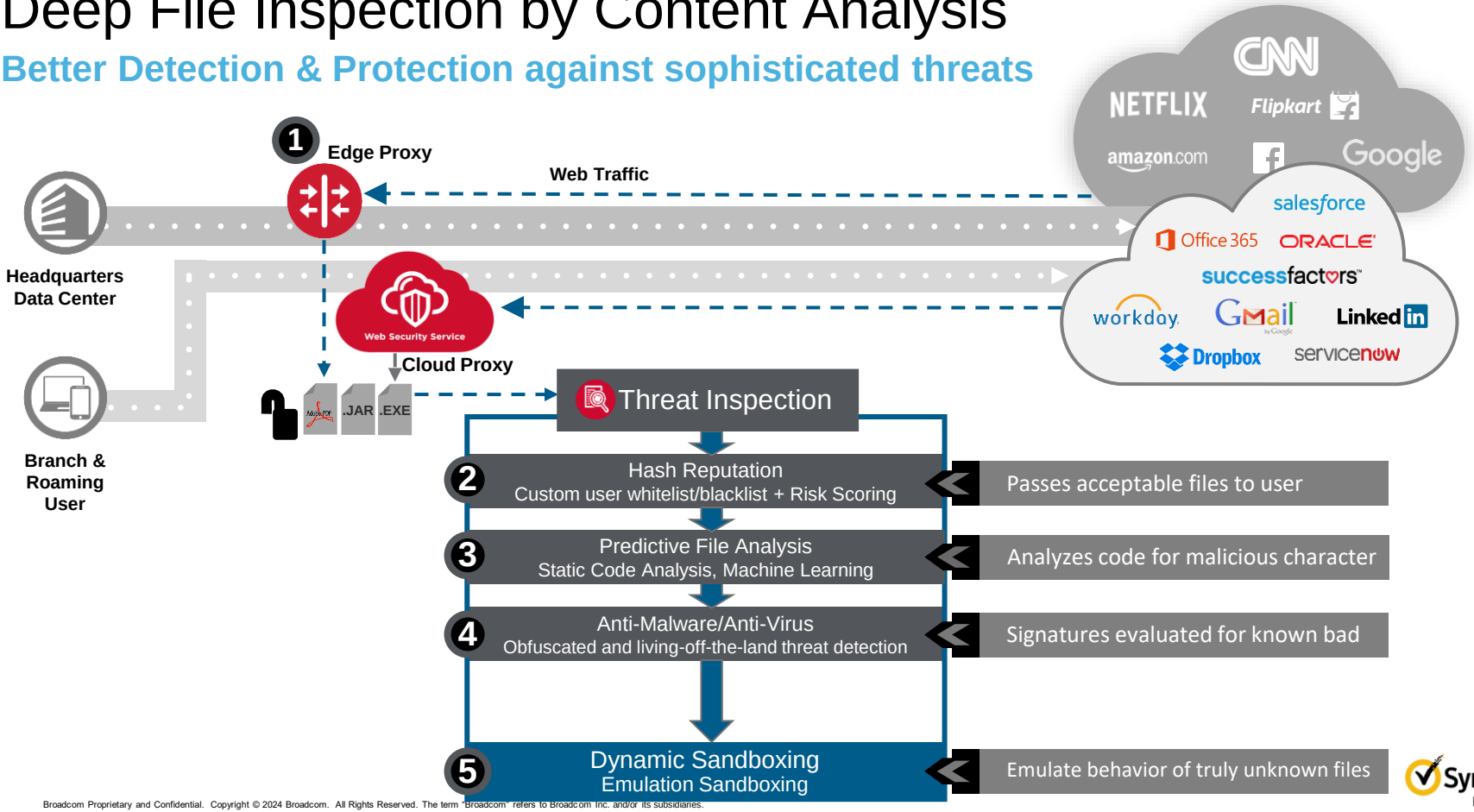
- **Proxy Service:** Web/Cloud App traffic gets deep proxy-based inspection & controls across all ports
- **Cloud Firewall Service:** Access and use controls for remaining internet

- **Improved Security & Performance**
  - Uniform policies follow your users
  - No backhaul to corporate data centers
- **Reduced Cost & Complexity**
  - Enables a secure “direct-to-internet” approach for branch offices
- **Full Visibility**
  - Centralized logging & reporting

Symantec by Broadcom

Deep File Inspection by Content Analysis

Better Detection & Protection against sophisticated threats



Symantec by Broadcom

總結

近期最常發生資安事件

- 加密勒索
- 資料外洩

法規遵循/合規性

- ISO27001:2022
  零信任框架
- CMMC 網路安全成熟度模型認證 (國防供應鏈)
- 上市上櫃資安管控指引

Symantec by Broadcom

關於 WESTCON TAIWAN

Westcon-Comstor 為全球領先的業務科技代理商，營運分佈於 70 多個國家/地區，將全球頂尖的 IT 廠商連結科技經銷商、系統整合商和服務供應商，創造業務價值和機會。

Westcon Taiwan 結合了對產業的洞察、技術知識和數十年的代理經驗，提供完整的解決方案，並且在邊界安全：防火牆/整合威脅管理、資料及網路應用程式安全、廣域網路加速/優化、商業分析、網路監控、管理與報表、虛擬化/雲端安全有深入的專門技術。

關於 Broadcom Symantec

Symantec以業界領先的專業技術面對全球最複雜的網路安全挑戰，包括封鎖未授權訪問、確保合規性，以及阻止企業面臨的最新攻擊。

我們支援各種平台，從移動設備到數據中心伺服器，並提供多種部署模式，包括本地、雲端和多雲。最關鍵的是，Symantec 確保您組織的關鍵數據和應用無論位於何處都安全可靠。從端點到網路，再到電子郵件和雲端，Symantec 致力於打造更安全的世界。

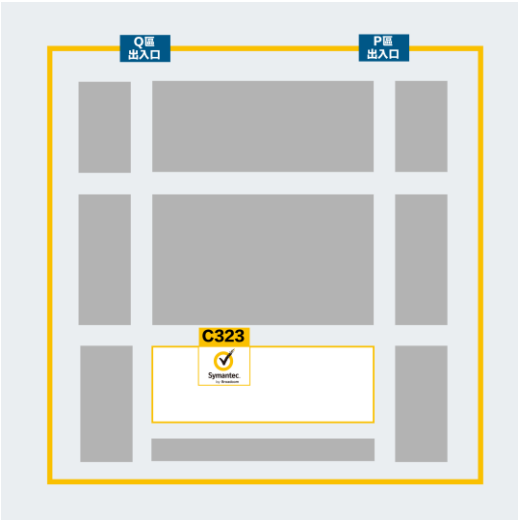
賽門鐵克 亞洲區 > 20個國家區域、澳洲、紐西蘭 獨家代理商

請立即掃描右方QR CODE
完成問卷賽門鐵克有好禮

今日憑問卷完成頁面至 1樓展場 No. 323 賽門鐵克展攤

第一重好康

兌換賽門鐵克限量版
多功能隨身LED燈



第二重好康

參加賽門鐵克幸運好禮抽獎活動即有機會可獲得
限量發行賽門鐵克口袋行動電源

感謝聆聽, 您的聲音我們最在意

Symantec 賽門鐵克, 我們一直都在!!