數位時代的資安航向：上市櫃企業營運資安保護關鍵策略

藍文贊 Bryan Lan
首席資深技術顧問, 亞太區

05/16/2024

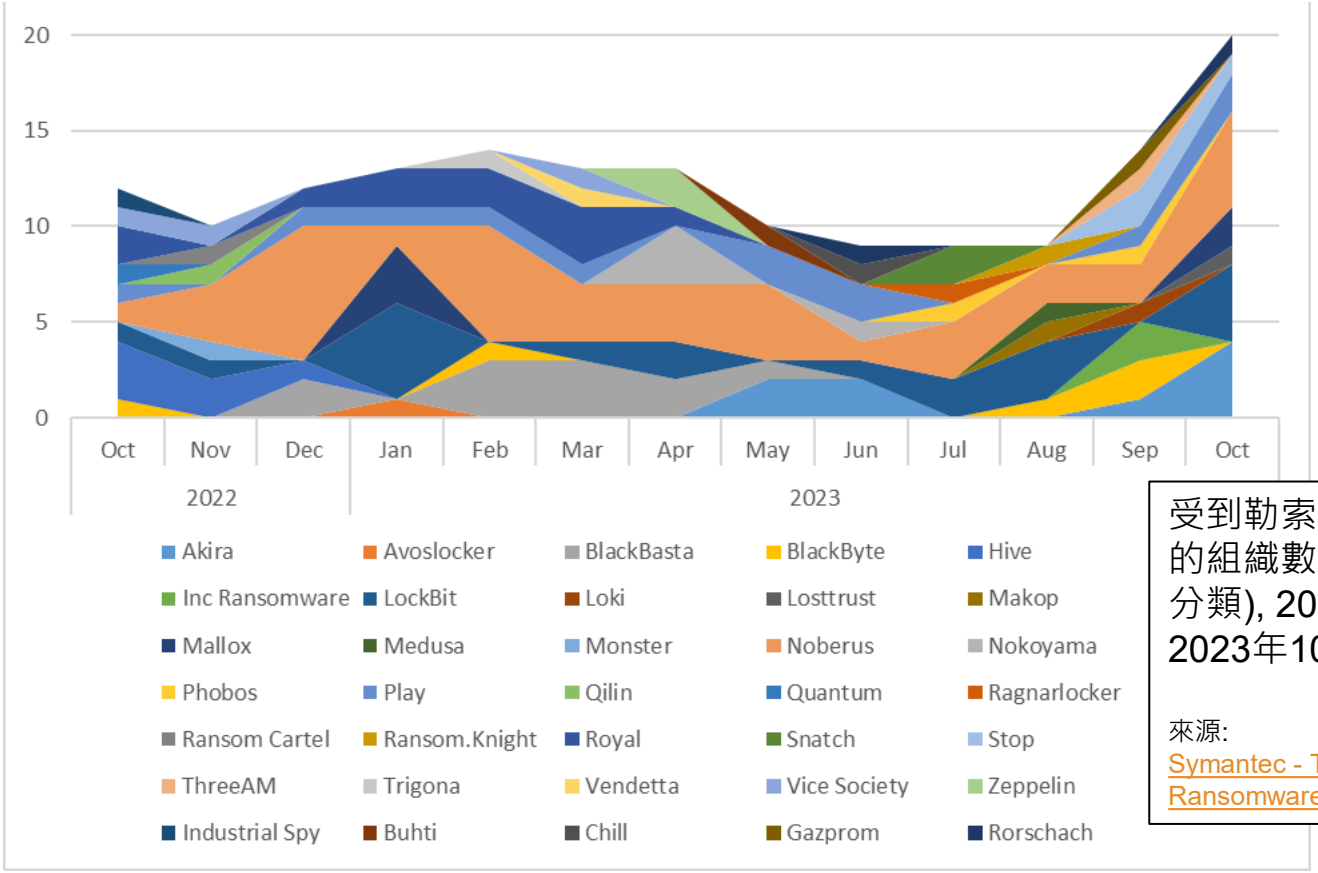
Agenda

1. 企業面臨的資安風險
   - 勒索軟體威脅上升
   - 企業使用VPN問題
   - AI帶來的資安風險
2. 賽門鐵克的防護策略
   - SES Complete
   - ZTNA
   - AI 防護
3. 賽門鐵克企業安全雲 (Symantec Enterprise Cloud)

Symantec by Broadcom

企業面臨的資安風險 - 勒索軟體威脅上升

2024勒索軟體威脅態勢



受到勒索軟體攻擊影響的組織數量 (依攻擊組織分類), 2022年10月 - 2023年10月

來源:
Symantec - The 2024 Ransomware Threat Landscape

Symantec by Broadcom

2024勒索軟體威脅態勢 – 分析

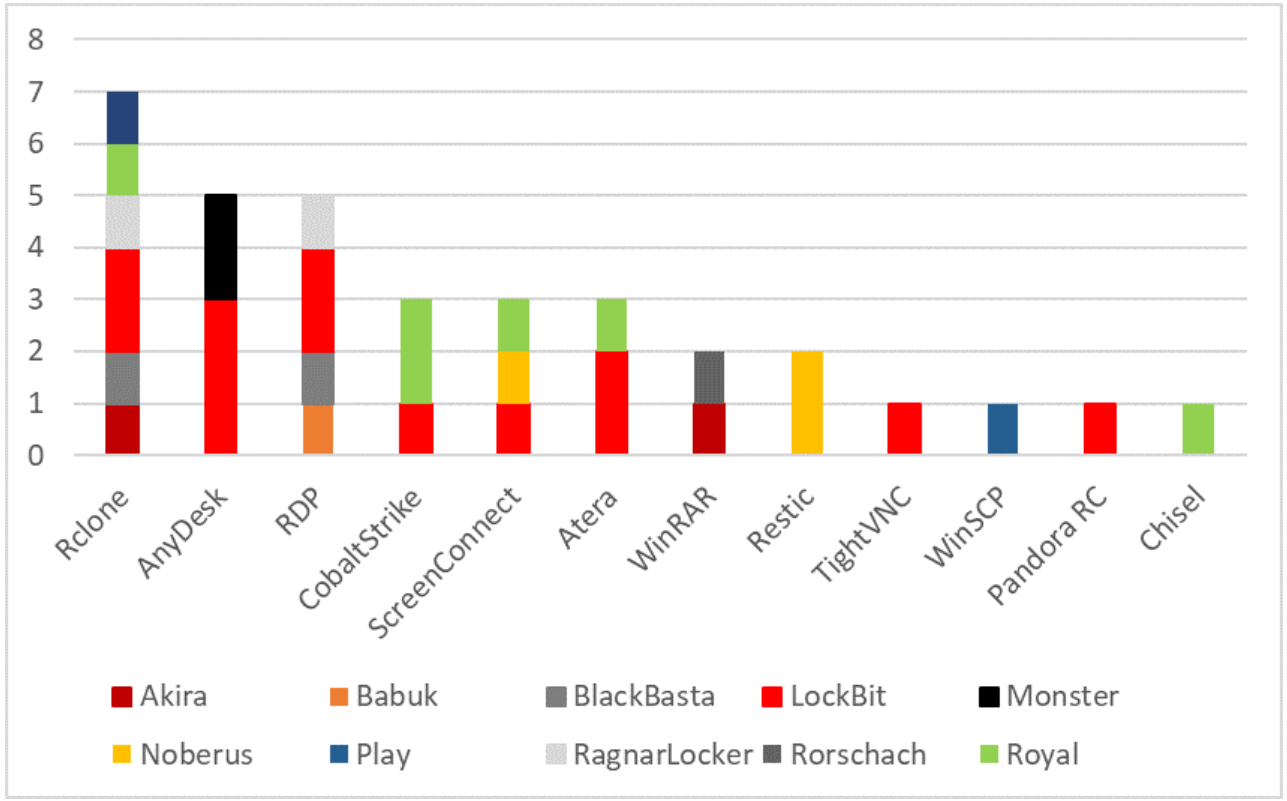
- 2023 年 10 月，受勒索軟體影響的組織數量比一年前增加了 66%。
- 勒索軟體的主要感染媒介不再是殭屍網路，而是利用面向公眾網路的應用程式中的已知漏洞。
- 除了勒索軟體自身的檔案外，攻擊者在實施攻擊時越來越多會避開惡意軟體掃描。

- Windows作業系統元件是使用最廣泛的合法軟體（"離地攻擊", Living Off the Land）。
- 遠端桌面/遠端管理軟體是攻擊者引入目標網路的最廣泛使用的合法軟體類型。
- Snakefly 組織（又稱 Clop）利用 MOVEit Transfer 漏洞展示了一種令人擔憂的勒索攻擊新模組。透過識別企業軟體中的零日漏洞，它可以同時竊取多個企業的資料。

參考: Symantec - Living off the Land

Symantec by Broadcom

勒索軟體攻擊組織常使用的工具



Symantec by Broadcom

2024勒索軟體的趨勢

- 勒索軟體不再只是北美的問題
- 攻擊者仍將持續利用軟體漏洞進行攻擊
- 加密貨幣不會很快消失
- 無加密攻擊呈現上升的趨勢

Symantec by Broadcom

企業面臨的資安風險 - 企業使用VPN問題

遠距工作將會是常態

41%

人力資源主管表示，員工可能會在疫情後兼職遠距工作[1]

74%

財務長打算將部分員工轉移到永久遠距辦公[2]

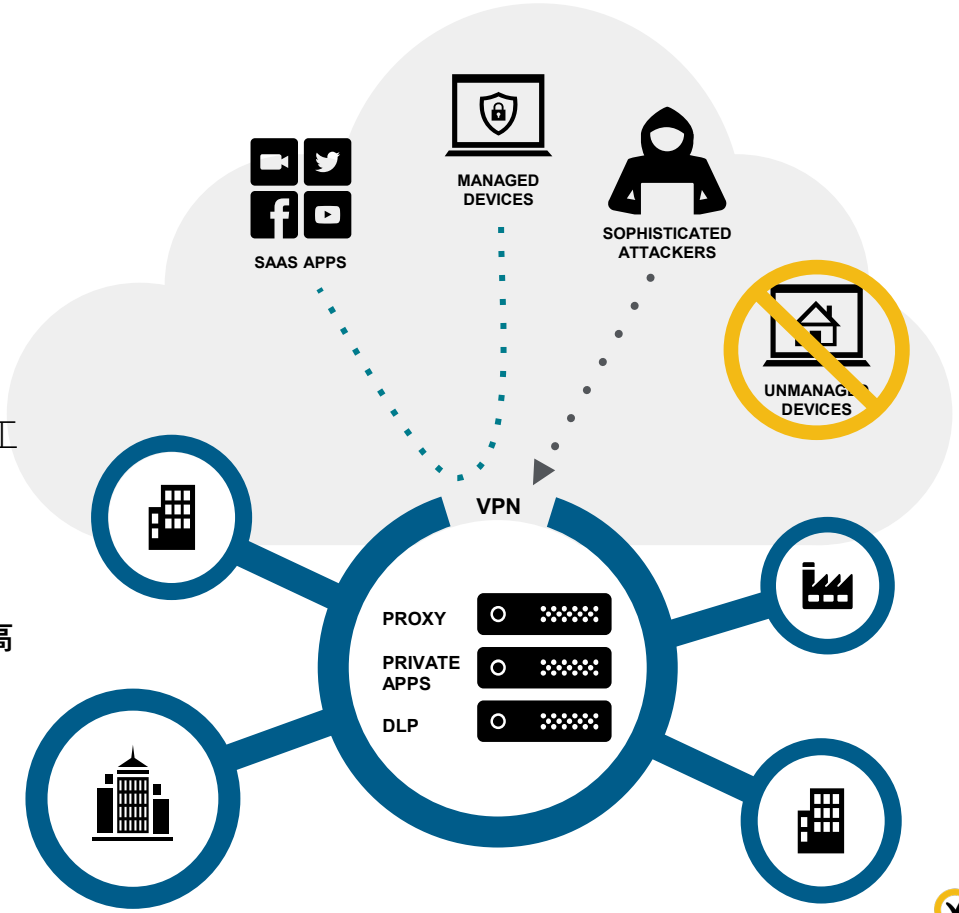
80% 的企業網路流量發生在企業的外部網路

[1] *Source: Gartner HR Survey*
[2] *Source: Gartner CFO Survey*

Symantec by Broadcom

傳統 VPN 問題

- 透過企業資料中心回傳流量的**低效率流量“髮夾(hairpin)”**
- 當只需要一部分應用程式時，VPN會授予**不安全的“完整網路存取權限”**
- **VPN 的擴充性不佳 -** 它們並非專為全遠距工作者而設計
- **只有受管控設備才能存取 -** 不支援 BYOD
- 管理企業範圍內的VPN支援的**營運成本很高**



Symantec by Broadcom

企業面臨的資安風險
- AI帶來的資安風險

生成式AI提高員工生產力

未受防護的使用會帶來重大風險

自動化效率

個人化的好處

優化的好處

創新機會

...伴隨著

資安問題

隱私問題

法律問題

整合問題

Symantec by Broadcom

AI在資訊安全的風險

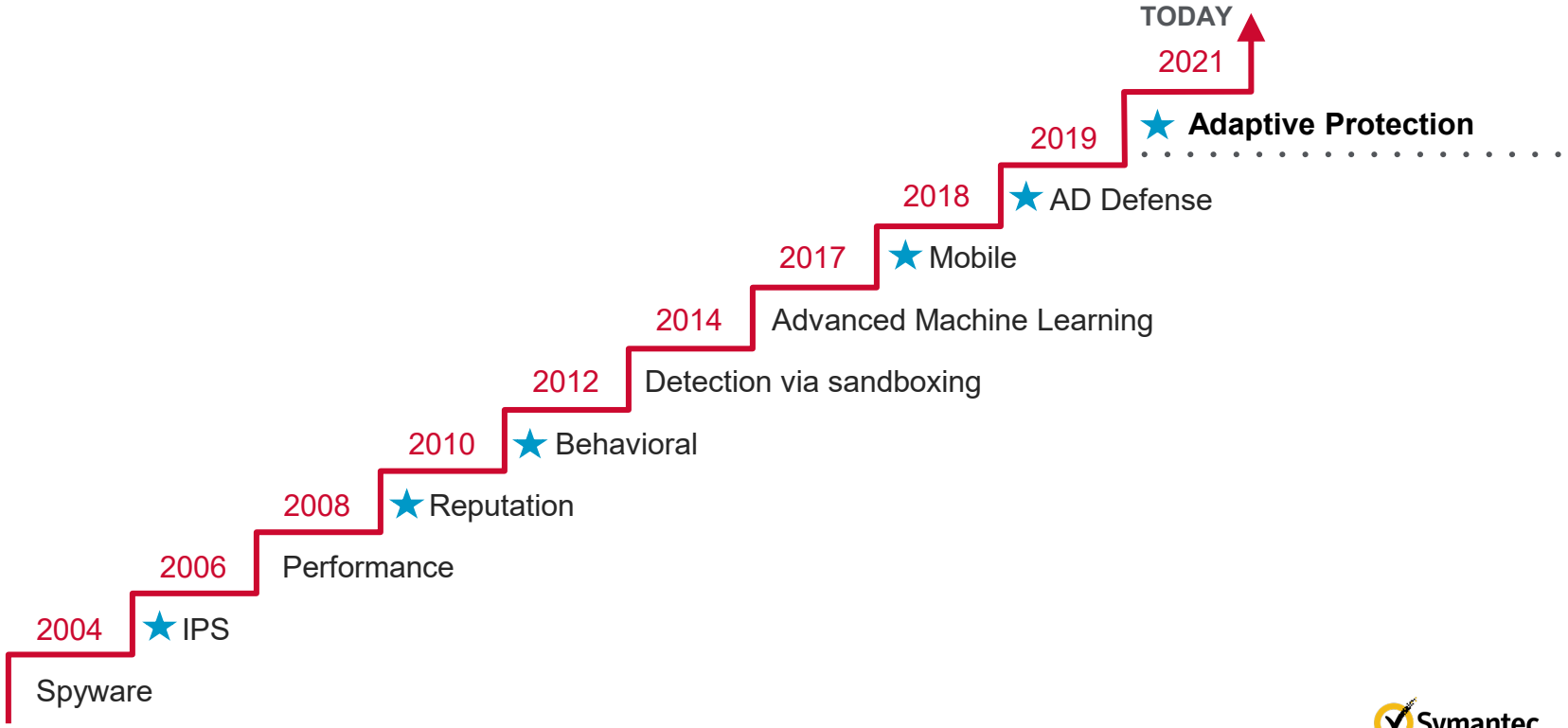
- **AI驅動的網路攻擊**
  - 自動魚叉式網路釣魚(spear-phishing)
  - 智慧型惡意軟體
  - 進階持續性滲透攻擊(APTs)與AI
- **利用AI系統**
  - 對抗機器學習(machine learning)
  - 模型下毒(Model poisoning)攻擊
  - 資料隱私洩露
- **生成式AI濫用**
  - 創造逼真的數位贋品
  - 隱私，版權、訴訟
  - 詐騙和身分竊取

Symantec by Broadcom

賽門鐵克的防護策略
- SES Complete

賽門鐵克端點防護(SEP)的創新之旅

透過創新與新附加的防護能力持續應對威脅情勢



Symantec by Broadcom

Symantec
Endpoint Security (SES) Complete

跨所有裝置和作業系統的業界最佳保護

Windows, Mac, Linux, iOS, Android, Windows 10S

- Endpoint Protection (SEP的進化版)
- Endpoint Detection & Response
- Threat Hunter & Threat Intelligence
- Adaptive Protection (調適型防護)
- Application Control (應用程式控制)
- Threat Defense for Active Directory

Symantec by Broadcom

SES Complete 涵蓋企業的關鍵安全問題

整合 MITRE ATT&CK 攻擊鏈的技術與創新

攻擊前 | 攻擊時 | 入侵時 | 入侵後

降低攻擊面

- Breach Assessment
- Device Control
- Application Control

攻擊防禦

- Machine Learning-driven Exploit and Malware Prevention
- Behavior-based Prevention
- Network Integrity, Wi-Fi Reputation, and Smart VPN

入侵防禦

- Deception
- Active Directory Defense
- Auto-managed Policies
- Network Firewall & Intrusion Prevention

偵測與回應

- Flight Data Recorder
- Behavioral Forensics
- Threat Hunter with Machine Learning and Expert Analysis
- Rapid Response

Adaptive Protection – Threat landscape insights, custom behavioral insights, and recommendations

Single Agent – all operating systems: Windows, Mac, Linux, Windows S Mode, Android, and iOS – including servers

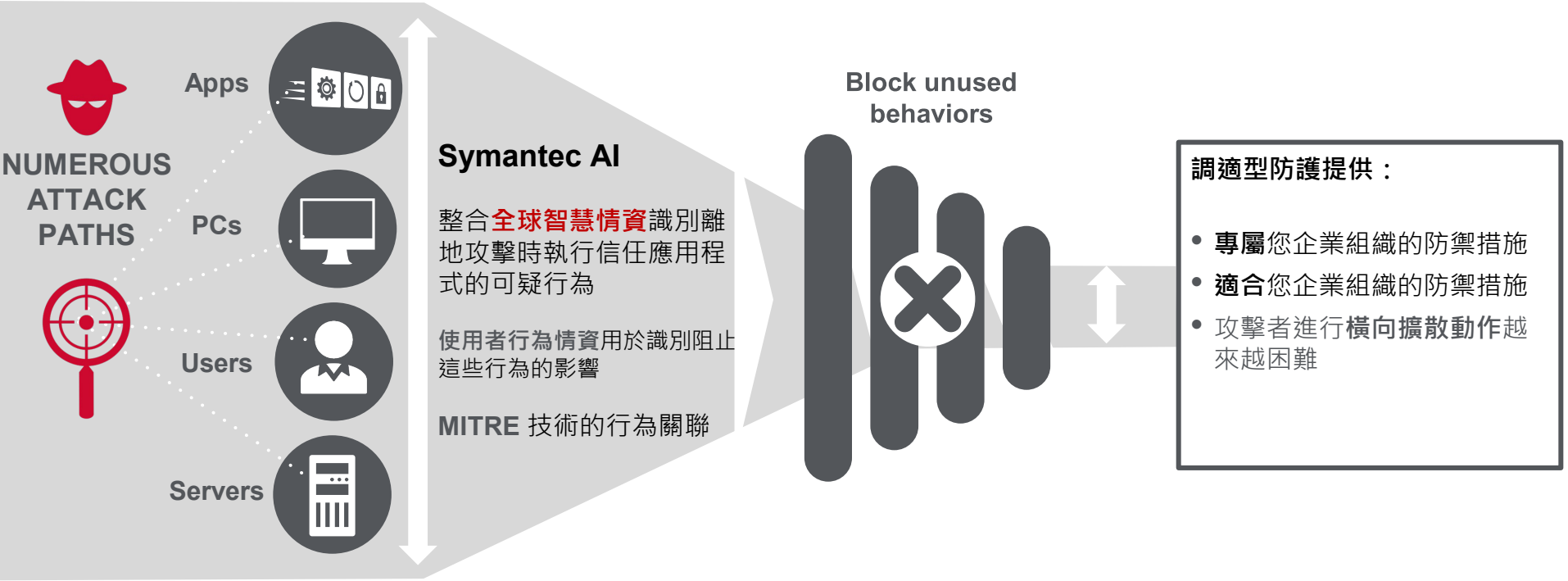
Global Intelligence Network – World's largest civilian cyber intelligence network

Integrated Cyber Defense – Enabling Symantec and third-party integrations

Symantec by Broadcom

Adaptive Protection (調適型防護) 防禦離地攻擊 (LOtL)

潛在的攻擊路徑

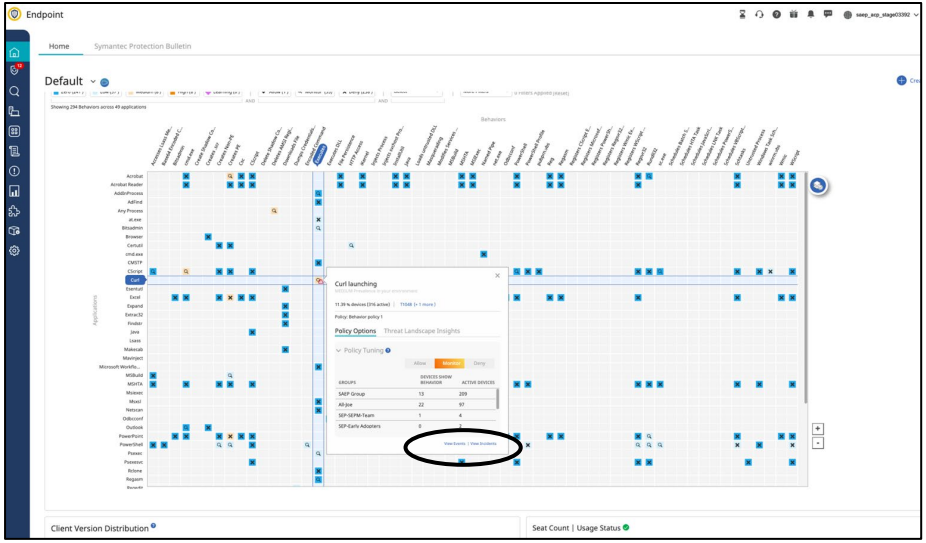


Symantec by Broadcom

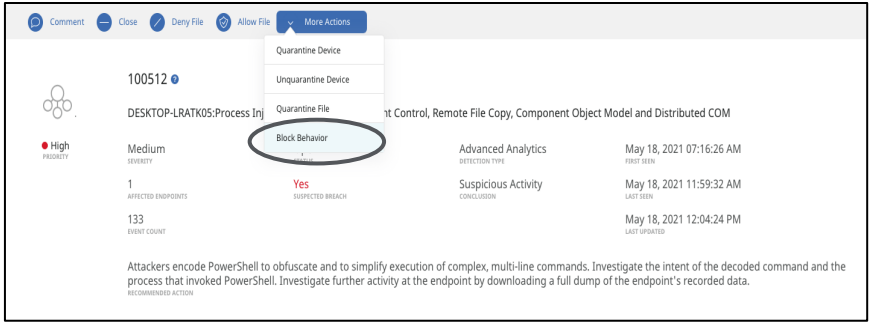
Adaptive Protection (調適型防護) 對應的偵測與防禦控管

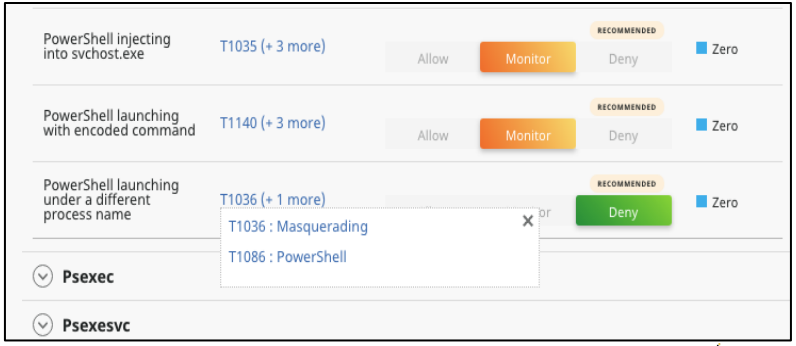
端點防護的 MITRE ATT&CK Framework

Most detections can be prevented



Granular policy-based controls to detect and block





Symantec by Broadcom

調適型事件如何運作

1

AI 技術評估由端點送來的事件

2

AI 技術比對環境中識別到與標記的**常見**事件

3 ADAPTATION

建立調適型事件並套用正常執行命令的規則

4

不尋常事件是可疑的；需要進一步的分析和調查

5

SOC 團隊看到的只是他們原本會看到的一小部分事件

Symantec by Broadcom

賽門鐵克的防護策略 - ZTNA

零信件網路存取 (ZTNA)

支援混合式安全及安全地取代傳統VPN

87% of Enterprises have a hybrid-cloud strategy

Flexara

96% of SASE adopters also plan to adopt ZTNA

ESG Research SASE Key Trends 2022

86% of SASE adopters are actively deploying ZTNA

ESG Research SASE Key Trends 2022

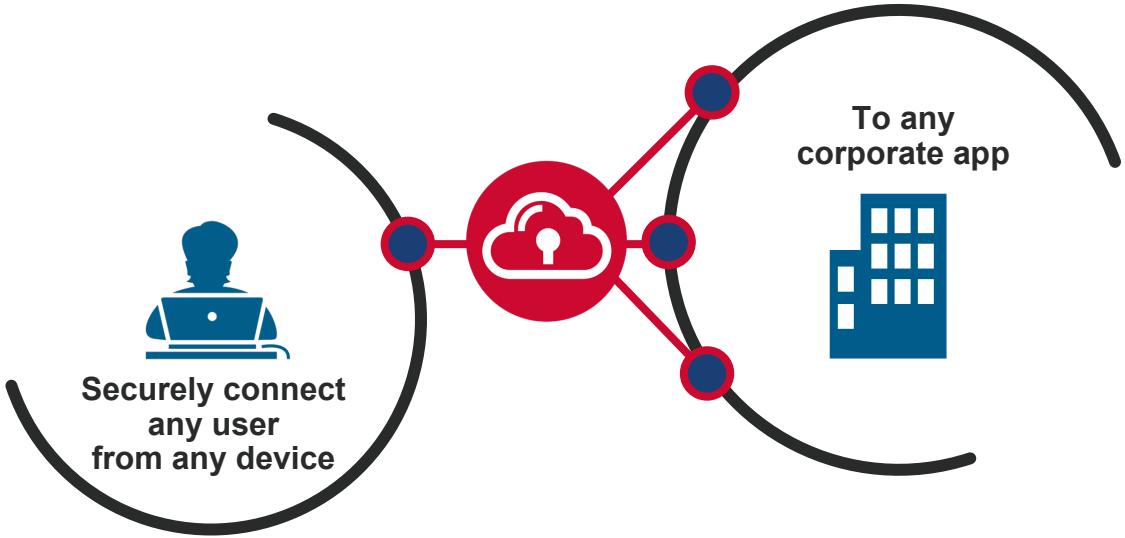
Symantec Zero Trust Network Access – point-to-point connectivity cloaks all corporate apps and resources, eliminating lateral movement and network-based threats

Symantec by Broadcom

ZTNA取代企業的VPN

Secure Access Cloud (SAC)

最小權限存取	Only direct access to apps users need – eliminating visibility and movement to other parts of the network
任何使用者, 任何裝置	Managed or Unmanaged / In or Out of the corp network – Support any user, any device
資料中心 或雲端應用程式	No VPN or partitioning needed for secure access to Data Center or Cloud-hosted apps
有端點程式 或無端點程式 **(AGENTLESS)**	Manage without agents or leverage Symantec Endpoint or Cloud SWG agents for instant deployment

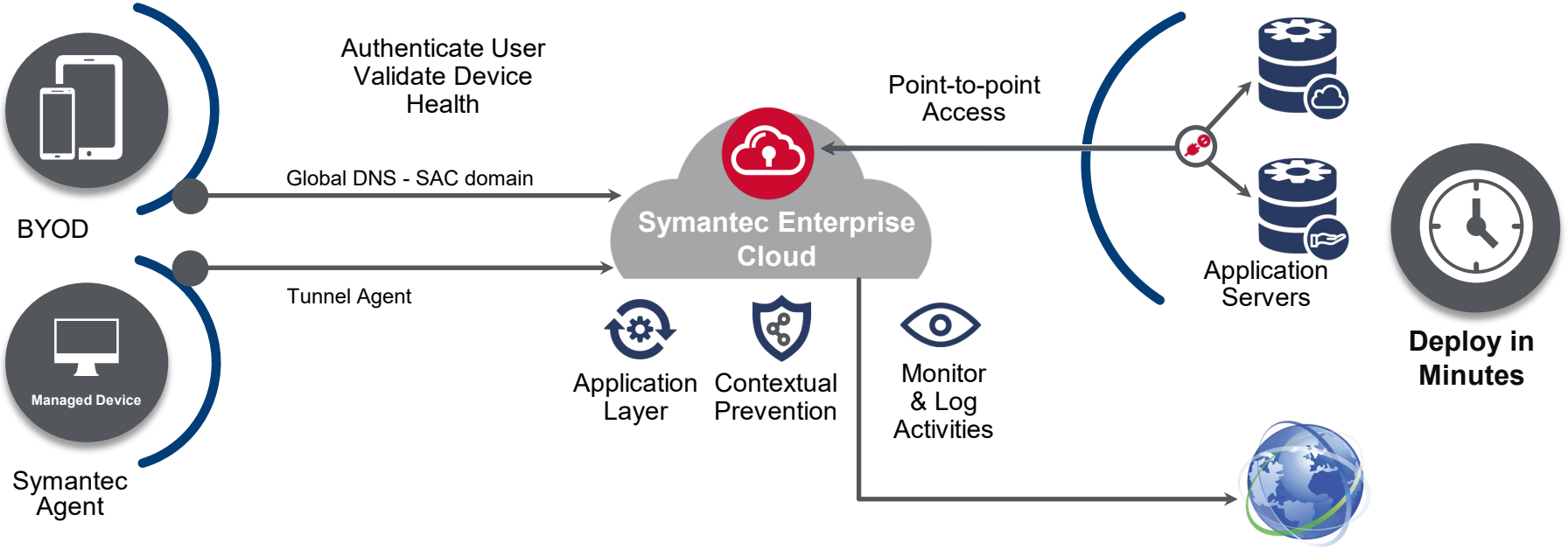


零信任存取：持續驗證使用者連線、限制存取的應用程式

Symantec by Broadcom

ZTNA如何運作

基於零信任的應用程式訪問



Anyone to anywhere – simple and secure app access

Symantec by Broadcom

賽門鐵克的防護策略 - AI 防護

防護AI濫用：工具與策略

政策和教育訓練 – 回歸基本

- 明確的AI使用政策 (並持續更新)
- 明確的資訊安全使用政策 (並持續更新)
- 定期員工教育訓練

存取控制和資料保護

存取控制
網路分段
資料加密
MFA, 生物辨識, 基於風險

雲端存取安全性代理程式(CASB)
資料外洩防護(DLP)
網頁代理(Web Proxy)
上網隔離(Web Isolation)

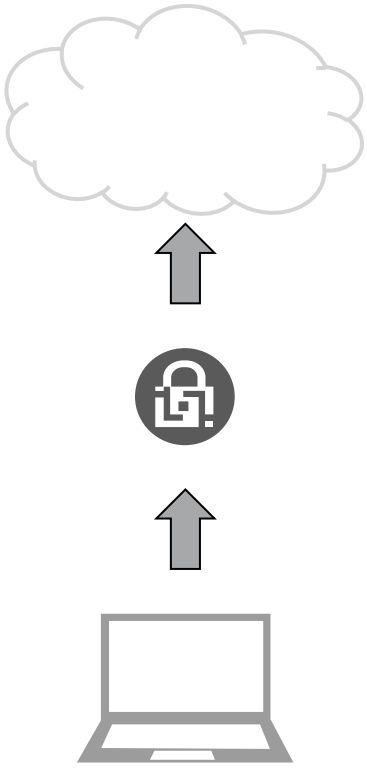
安全措施及維護

安全開發實務
更新和修補程式
端點安全

威脅偵測與回應
威脅情資
定期威脅評估

Symantec by Broadcom

賽門鐵克多層次的威脅/資料檢測及安全防護



Custom Gatelets	(Blocking, PUT/POST/File Uploads Content Inspection)	DLP Cloud CloudSOC (CASB)
CASB Audit / Shadow IT	(Activity Monitoring)	
SSL Interception	(Blocking, PUT/POST/File Uploads Content Inspection)	Network On Prem Proxy > ICAP > Web Prevent -or- Off Prem WSS > DLP CDS
On Device Content Inspection	Paste - File Uploads - Supported Browser Inspection (** Disable 'guest' profiles)	DLP Endpoint Agent
On Device URL Blocking	URL Intelligence. Allow / Block lists	SEP / SESC / WSS Agent

Symantec by Broadcom

生成式AI防護

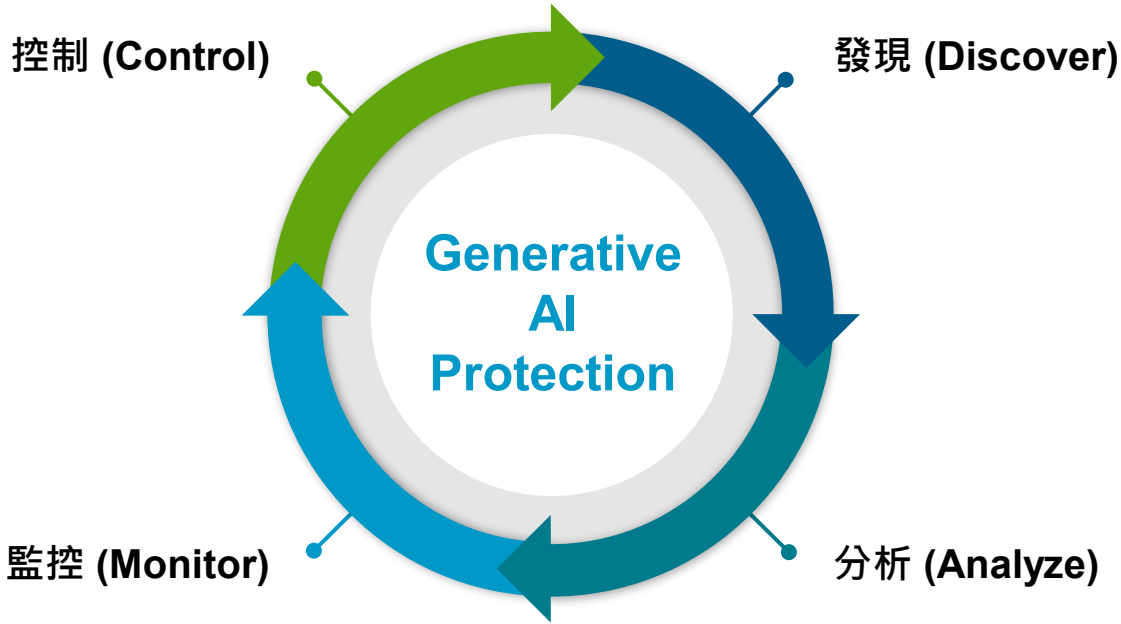
解決各式風險偏好的實務

	保守型			積極型
企業傾向使用生成式AI	我們不使用生成式AI，我想阻擋所有的連線	幫助我們了解生成式AI的風險	我們需要嘗試一下，如何才能創造一個安全的「使用環境」？	我們計劃廣泛使用生成式AI，如何防止資料外洩？
賽門鐵克生成式AI防護	● 阻擋所有AI類別的網站及衍生網站 ● 透過Shadow IT的稽核，發現未經授權的使用	● 展示您組織中的使用情況 ● 評估生成式AI應用程式的安全狀況	● 限制僅存取受信任的生成式 AI 應用程式 ● 套用基於角色或風險的存取控制	● 根據 DLP 政策檢查所有內容 ● 套用監控、警告使用者或阻擋規則

Symantec by Broadcom

透過賽門鐵克保護您的AI使用

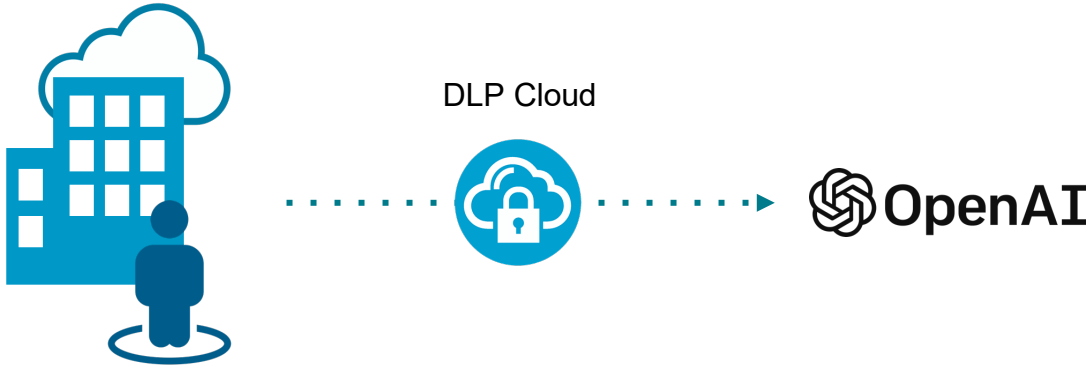
DLP Cloud提供生成式 AI 防護



Symantec by Broadcom

發現(Discover)組織內使用的AI apps

識別正在使用的已知 GenAI 應用程式以及使用它們的使用者



提高可視性
Discover the Generative AI apps used within your organization

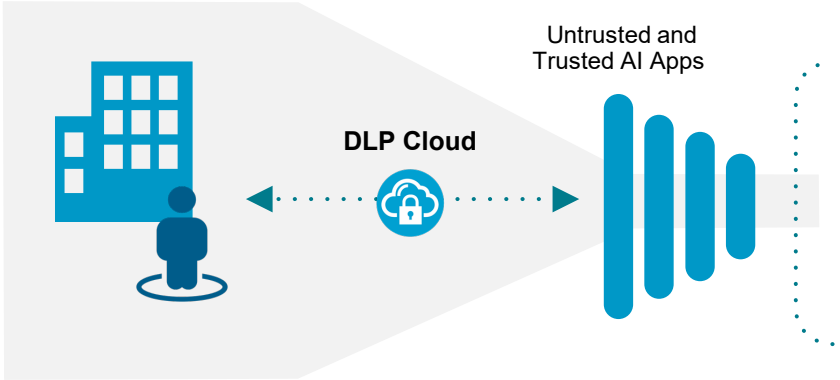
識別使用者
Hone-in on the individuals using specific apps in your organization

瞭解共用的資料
Understand the amount of data being exchanged which provides usage patterns

Symantec by Broadcom

分析(Analyze)生成式AI apps的風險

透過300+研究屬性和風險因素評估風險



Trusted AI Apps

ChatGPT Bard AI DALL·E 2

25+
Generative AI apps in the catalog

300
Risk attributes and risk factors

識別風險
Assess the risk of the discovered apps, based on Symantec *Business Readiness Rating* against 100+ risk factors, including legal, regulatory & security.

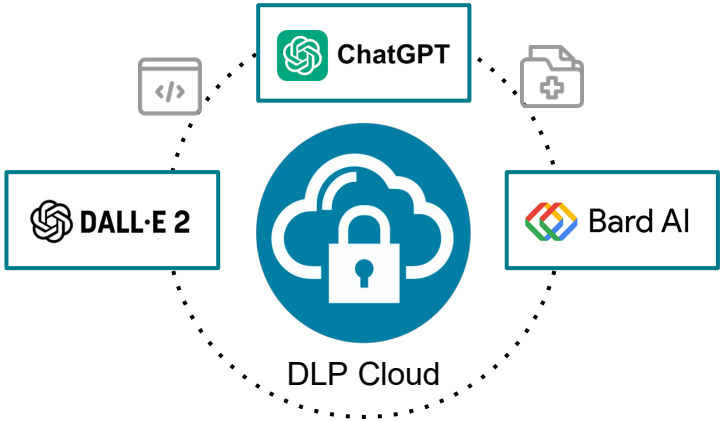
評估合規性
Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR, HIPAA

分析和資料分類
Analyze usage, risk and compliance data to prioritize the sanctioning and un-sanctioning of generative AI apps. An executive report gives a summary overview and recommendations.

Symantec by Broadcom

即時監控(Monitor)app使用情況

使用屬性，例如使用者、地點、設備資訊和共享資料



識別並追踪應用程式連線

Continuously monitors generative AI app usage.

監控資料傳送到AI應用程式

Monitor and inspect data in motion to generative AI apps. Highlight any risks and compliance issues these may pose.

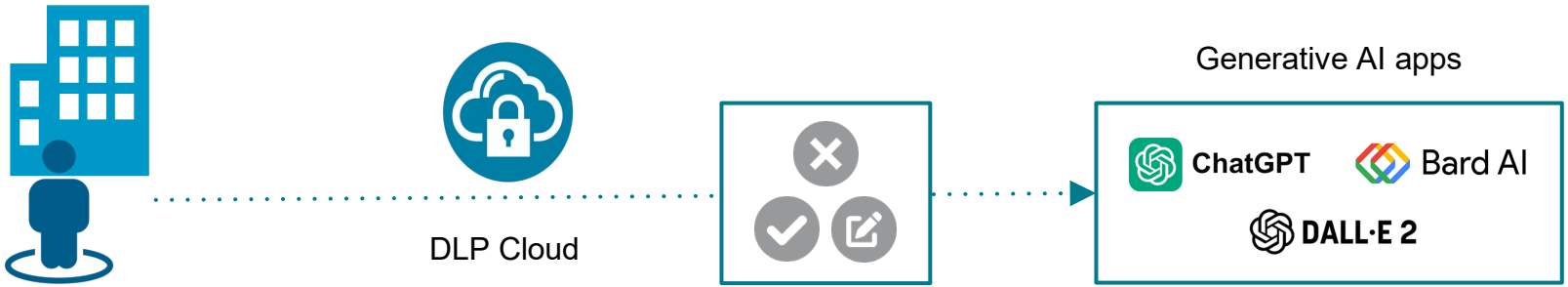
調查DLP事件

Investigate and correlate with users' activities through native UEBA

Symantec by Broadcom

控制(Control)生成式AI app的使用

提供即時使用分析並根據需要進行調整



控制存取AI應用程式

Block unapproved AI apps while allowing access to those that meet security guidelines. Add apps from Audit to CASB Gateway or use AppFeed integration with Edge and Cloud SWG, and apply granular policy controls.

防護機敏資料

Detect sensitive content with DLP policies and prevent data transfer Extend existing DLP policies to Generative AI apps

套用自適性政策

Use User risk scores in DLP policies (Adaptive Risk-based Policies) to further reduce risk posture.

Symantec by Broadcom

了解生成式AI防護的價值

賽門鐵克如何解決您面臨的挑戰

防護經由生成AI的資料傳送

Shadow IT: 發現公司政策未批準的應用程式

阻擋未批準的應用程式

阻擋與AI相關的未分類、可疑或有風險的活動

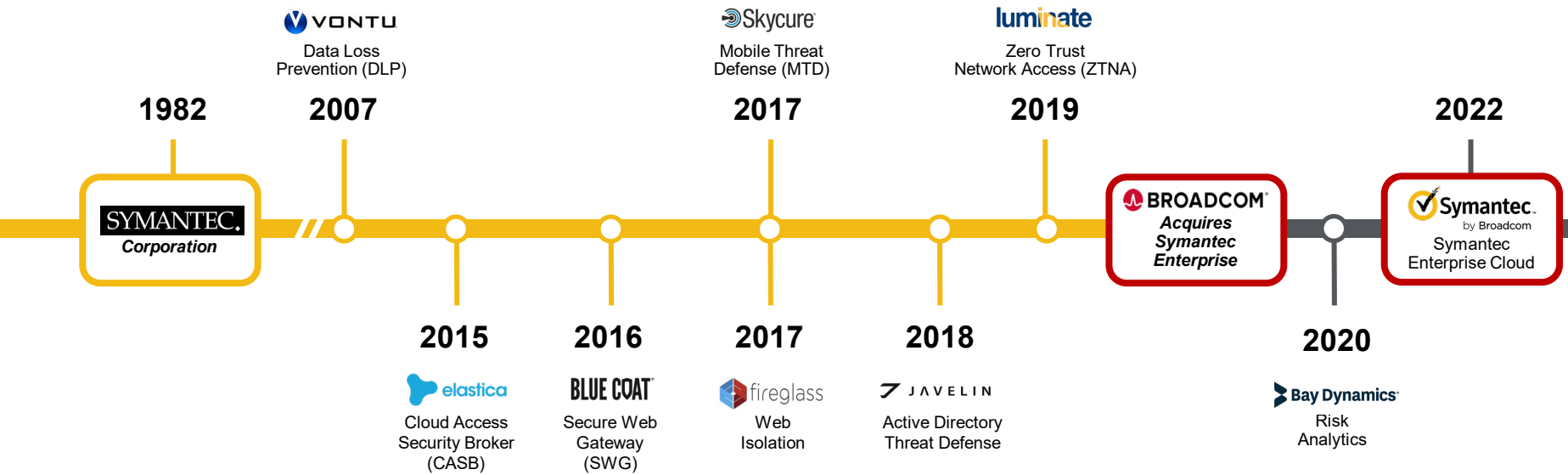
符合公司治理與法規遵循的要求

Symantec by Broadcom

賽門鐵克企業安全雲
(Symantec Enterprise Cloud)

賽門鐵克為滿足最新資訊安全需求而不斷發展

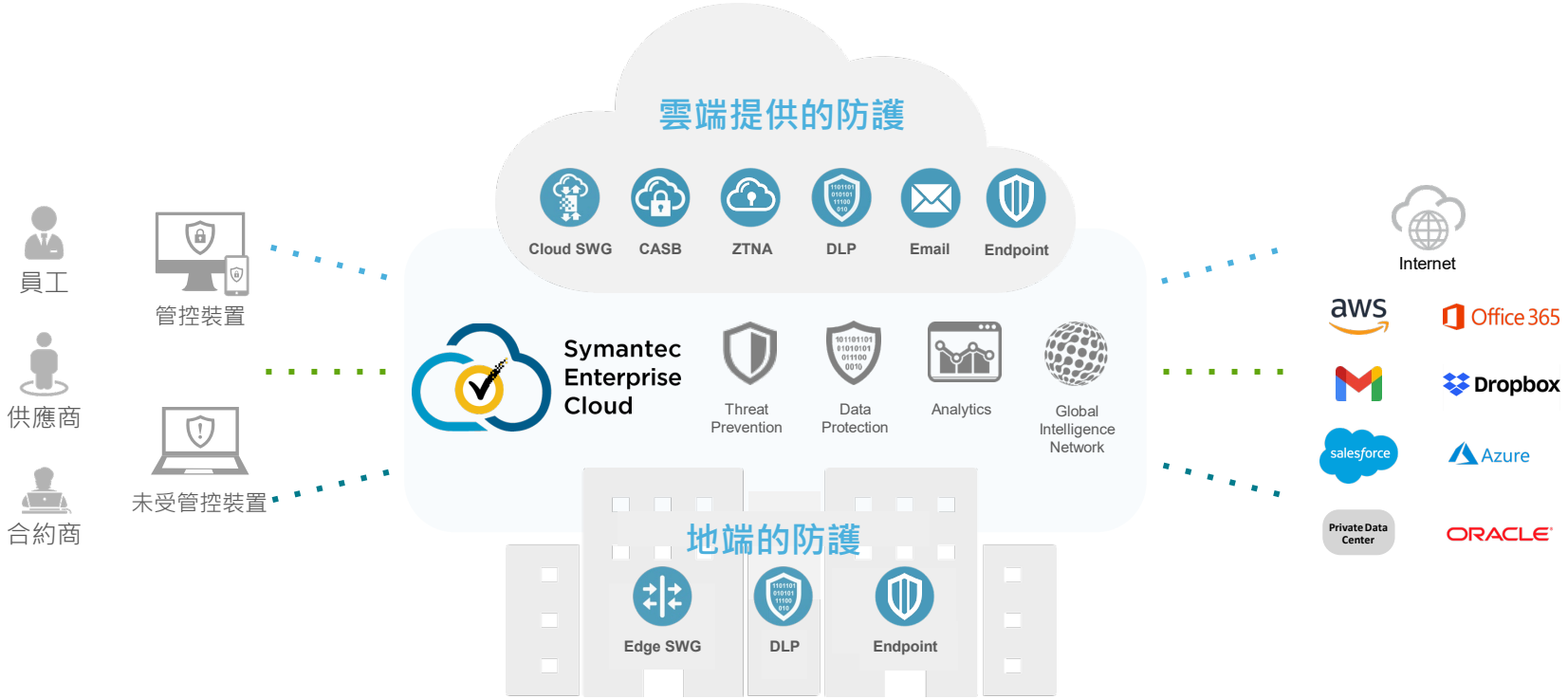
多年來建立和優化廣泛而深入的技術能力



Symantec by Broadcom

創新：將產品轉變為有遠見的解決方案

賽門鐵克提供以資料為中心的全面資訊安全防護



Symantec by Broadcom

Thank you