Symantec
by Broadcom Software

白皮書

# 驅動網路安全創新的未來

白皮書

# 驅動網路安全創新的未來

Symantec by Broadcom Software

## 目錄



## 執行摘要


賽門鐵克夠創新嗎？這是一個蠻有道理的疑問，這個疑問的答案，其實遠比許多人以為的要簡單。尤其當資本市場對新創公司的追捧，人們很容易得出結論說創新技術只能由最火紅的新創公司創造時。事實上，賽門鐵克40年的歷史一直專注在安全性整合以及堅持其解決方案在企業內部和雲端環境中的工作，都使其不符合資本市場的「創新者」的標準。自從2019年被Broadcom®收購後，更加專注在世界上要求最嚴苛的大型企業組織的銷售，大家很容易將賽門鐵克視為另一個緩慢發展、等時機被顛覆的大型企業。

就廣義來看，賽門鐵克一直持續在創新：透過創造、精挑細選、收購、開發和整合安全技術；並且事先設想好須符合如零信任和安全存取服務邊緣 (Secure Access Service Edge，SASE) 等安全框架規範。賽門鐵克以多種形式持續進行創新：

- **重新設計**安全軟體，使其在全球首屈一指的高性能、低延遲的邊緣網路--Google Cloud上運行。
- 解決全球企業面臨的合規性、整合、居家辦公和多雲環境問題的**產品進展**情況。
- **業務創新**，例如：統合簡化定價策略，更具吸引力的依使用者計價模式為賽門鐵克客戶提供最靈活的部署。
- 為了代表客戶的利益，與產業、政府和監管機構合作進行**標準創新**並開發不受任何限制皆可操作的解決方案。

最新一輪的創新是賽門鐵克企業安全雲 (SEC：Symantec Enterprise Cloud)，這是一個具高度集合與統整能量的混合雲解決方案，在賽門鐵克安全營運中心 (SOC) 全球網路支援下提供資料和威脅保護。作為融合零信任原則的安全服務邊緣 (SSE) 的超集合，SEC為最複雜和最廣泛的企業網路提供端到端安全解決方案。

賽門鐵克持續創新，代理整合的長期目標現在已經實現。賽門鐵克單一代理從技術、平臺和環境，對合規性、安全遠端工作和網路安全等多面向提供周全且一致的管理，沒有遺漏或重疊。

**賽門鐵克一直在創新：透過創造、收購、整合和擴展網路安全解決方案，並且事先設想好須符合如零信任和安全存取服務邊緣(Secure Access Service Edge，SASE)等安全框架規範。**

## 賽門鐵克如何創新

即將邁向第五十年頭的賽門鐵克被公認是最穩健的網路安全領導者，長期商譽卓越。作為博通公司的成員，賽門鐵克的戰略已經從每季度的產品銷售收入調整為與世界傑出公司的長期合作。這些客戶對賽門鐵克有很高的期望，但他們應該期待創新？

本文將以實證成果與可實現的願景陳述賽門鐵克的持續創新：透過創造、收購、整合和擴展網路安全解決方案，並且事先設想好須符合如零信任和安全存取服務邊緣(Secure Access Service Edge，SASE) 等安全框架規範。自 2019 年被博通收購以來，賽門鐵克繼續加強和整合關鍵的安全技術，除同時重新建構在 Google Cloud 雲端基礎設施上的所有安全解決方案，並增加其研發投資。也在業務流程方面進行創新，對產品進行擴展、捆綁和簡化定價，以滿足大型及全球不同規模之企業組織的要求。它的創新也表現在與全球範圍內的政府、監管機構和標準組織的合作，並領航全球安全技術的發展。將這些技術與賽門鐵克企業雲結合起來，這是一個全方位的解決方案，可以滿足大型企業期盼的以資料為中心、跨平臺的安全。

## 透過收購的創新：賽門鐵克1989~2019

賽門鐵克成立於 1982 年，自 1989 年上市以來，積極物色和收購那些開發出有利基點且後勢看好的安全技術公司來擴展其網路安全業務。由於這些新創公司通常缺乏所需的資源，賽門鐵克擔任將其單一解決方案發展為功能更齊全且滿足市場需求解決方案的角色，並使其與其他安全技術相容或整合。表 1 概述賽門鐵克「收購、開發和整合」戰略的要點。

如表所示，這些收購不僅僅是為了提高營收而選擇的單一解決方案。它們在單一產品過時後被整合到更廣泛的產品中，或被擴展到多個平臺上，還能繼續增加價值。

**表1：賽門鐵克的收購以及來自收購的創新：1989－2019**

| 原公司 | 技術領域 | 革新／進化的貢獻 |
|---|---|---|
| Certus | 病毒防護 (AV) | 更新、擴展並整合到賽門鐵克端點安全完整版(SESC)--Radicati 集團連續七年的排名最高的廠商。 |
| Vontu | 資料外洩防護 (DLP) | 賽門鐵克資料外洩防護核心和雲端解決方案的基礎--是 2021 年 Forrester Wave 在相關領域的領導者。 |
| Elastica | 雲端存取安全中介 (CASB) | 更新、擴展，並作為控制點整合到雲端版的資料外洩預防 (DLP)。 |
| Blue Coat | 安全網頁閘道 (SWG) | 可作為雲端遞送的網路安全服務，具有廣泛的選項和整合性--SWG 技術的長期領導者。 |
| Skycure | 行動裝置威脅防禦 (Mobile) | 整合到賽門鐵克端點保護行動裝置版本中，實現了尊重用戶生產力的高預測能力、多層次的行動裝置防禦。 |
| Fireglass | 網頁隔離 | 融入賽門鐵克雲端安全網路閘道，允許未受控管的裝置安全存取雲應用程式。 |
| Javelin | AD 威脅防禦 | 整合到賽門鐵克端點安全完整版(SESC)中，以混淆技術強化 AD 防護，阻止管理員憑證被盜。 |
| Luminate | 零信任網路存取 (ZTNA) | 可作為賽門鐵克安全存取雲，是存取私人應用程式的安全雲閘道。 |
| Bay Dynamics | 訊息中心的分析 (ICA) | 將訊息中心的分析 (Information Centric Analytics ICA) 用戶風險納入 DLP 策略中。 |

## 框架與架構

賽門鐵克收購、開發和整合安全技術，以有效應對新興威脅（資料洩露、勒索軟體）和保護新平臺（行動裝置和雲端）。與此同時，分析公司正在梳理與匯整這些新的電腦環境所需採取的對應行動，並為其防禦推薦架構和框架。這些基本上都是針對同一問題的商業性和分析性的觀點，所以它們被一起討論一點也不奇怪：賽門鐵克的技術完全符合分析師的要求，而且在某些情況下還有先見之明。零信任安全架構和 SASE 技術就是最明顯的例子。

### 框架與架構

行動裝置和雲端平臺等新科技的開發和採用逐漸侵蝕傳統網路防禦的「安全邊界」模式。新一代是一個無邊界、以資料為中心的安全架構，稱為零信任。零信任的底層邏輯是驗證任何試圖存取資料的人、設備或工作負載，無論其物理位置、網路位址或存取方法如何，只指派與被驗證實體相關的存取權限。零信任需要自動化和一體適用的統合性，以便每個組成技術都可以順暢協作，並需要可見性和分析來監測、控制和管理架構。

早在 2009 年權威獨立研究機購 Forrester Research 研究公司提出零信任模式之前，賽門鐵克就已經匯整、開發並提供了實作該架構所需的每一項技術，並以身分治理(Identity Governance)和管理解決方案為後盾，對用戶存取進行自動審核和認證。

早在美國國家標準與技術研究院 (National Institute of Standards and Technology，NIST) 定案 SP 800-207 準則之前，賽門鐵克已經採取進一步措施，將零信任技術併入其新興的雲端解決方案系列：

- **安全存取雲**，一個零信任網路存取 (ZTNA) SaaS 解決方案，管理對部署在資料中心或 IaaS／PaaS 雲端的應用程式的存取。
- **賽門鐵克 VIP** 基於雲的多因素憑證和情境脈絡風險分析適用於未受管理的設備。
- **以零信任為中心的資料功能**內置於賽門鐵克安全網路閘道、CASB、端點和電子郵件解決方案中，由整合的賽門鐵克 DLP 支援。

**賽門鐵克收購、開發和整合安全技術，以有效應對新興威脅和保護新平臺。**

### 安全存取服務邊緣 (Secure Access Service Edge，SASE) 技術

SASE 技術是由 Gartner 分析師於 2019 年全新定義快速可靠的網路架構及安全服務的框架，作為直接給網際網路邊緣用戶的雲端服務。SASE 承諾提高網路和應用程序性能、增強安全性、降低複雜性並減少成本。一個主要優勢是它避免透過集中式資料中心回傳所有流量的負載和延遲，例如：虛擬私人網路 (VPN) 就是這樣。2021 年，Gartner 為提升 SASE 的更完整性，特別定義更細部的安全服務邊緣 (SSE：Secure Services Edge) 技術。

與零信任一樣，在SASE正式成為網路架構框架的第一時間，賽門鐵克就能提供這些目標所需的關鍵技術。表 2 說明了賽門鐵克技術完全符合 Gartner 所定義的 SASE 框架，並經第三方公正單位 Tolly Enterprises，LLC 驗證。

如果與框架不完全符合，通常是因為賽門鐵克包含原始框架中未充分描述的技術（例如：保護儲存中的資料）或環境（例如：地端）。

**在零信任和SASE正式成為網路架構框架的第一時間，賽門鐵克就能提供這些目標所需的關鍵技術。**

表 2：Symantec SASE 技術

| 框架元件 | 功能區域 | 對應的解決方案 |
|---|---|---|
| 安全網頁閘道（SWG：Secure Web Gateway) | Secure Web Gateway<br>- 網頁威脅防護及分類<br>- 進階內容分析(惡意軟體沙箱) | Symantec Web Protection |
| CASB | 雲端存取安全中介--Cloud Application Security Broker (CASB) | Symantec DLP Cloud |
| ZTNA/VPN | 零信任網路存取<br>(ZTNA-Zero Trust Network Access) | Symantec Secure Access Cloud |
| FWaaS(防火牆即服務) | 雲端防火牆(Cloud Firewall) | Symantec Web Protection |
| 遠端瀏覽隔離<br>(Remote Browser Isolation) | 遠端瀏覽隔離<br>(Remote Browser Isolation) | Symantec Web Protection |
| Decryption(加密流量安全) | SSL 加密流量檢查功能<br>(SSL Inspection) | Symantec Web Protection |
| 資料外洩預防<br>(DLP:Data Loss Prevention) | 資料外洩預防<br>(Data Loss Prevention) | Symantec DLP Cloud |

來源：Tolly Enterprises LLC 報告 #222122，2022年7月

## 博通收購賽門鐵克企業部門

2019 年 11 月，Broadcom 收購賽門鐵克 (Symantec Corporation) 的企業安全部門，朝著公開聲明的目標前進「……在我們全球核心的 2000 大客戶群中擴大我們關鍵任務基礎設施軟體的市場。」

併購賽門鐵克企業安全業務，並不包含其原先的小型企業和 Norton (諾頓) 消費者產品線—過去和現在都符合 Broadcom 專注全球規模最大企業的戰略。正如側邊欄所示，賽門鐵克解決方案有這個意願也有能力投入更多資安投資的高端市場中的滲透率非常高，並且後勢大有可為。

## 賽門鐵克企業市場滲透率

－《財富》世界500強有**195**家

－全球前2000大企業有**697**家

－全球前13大銀行**全都是**

－全球前10大電信公司有**8**家

－全球前10大汽車製商有**7**家

－全球超過 **1.5 億**個企業用戶

## 博通收購賽門鐵克企業部門(續)

此次收購對賽門鐵克的戰略產生了巨大影響。持續創新的長期成長策略取代對季度營收錙銖計較的短視近利是主要的關注重點，資源重新配置從開發新客戶轉變成幫助老客戶成功且更有效益的諮詢和支援提供。

與市場行銷和銷售資源等同重要，創新被組織起來以增進 Broadcom 全球客戶群的利益，重點專注在這些客戶最重要的領域：

- **法規遵循：**是大型跨國公司的主要推動力，並且隨著新監管機構的堅持和舊監管機構在區域內的分散而快速增長。
- **整合：**整合一直是大公司的首要任務，現在透過將賽門鐵克解決方案與 Broadcom ValueOps™、AIOps 和其他企業軟體整合的機會得到增強。
- **工作無所不在：**疫情大流行後的既定事實，要在並非為此設計的傳統基礎設施之上構建安全高效的使用者體驗是極為嚴峻的挑戰。
- **混合和多雲環境：**地端基礎設備已經過時，但資料所在位置和資料安全問題使大多數跨國公司無法全面採用雲端技術。

在Broadcom收購之後，新產品上市的訊息和公關新聞稿發佈的步伐有所放緩，許多分析師認為賽門鐵克在創新方面已經「黯然失色」。但這個時期實際上是其歷史上最繁忙、生產力最高和最具創新性的時期之一，因為賽門鐵克在雲端中重建其整個安全基礎架構，以滿足其全球客戶的需求。

## 收購後的創新

Broadcom收購之後，大家很快意識到，要以高效能的方式從雲端為企業客戶提供服務，賽門鐵克需要重新構建其雲端產品組合平台。

### 與 Google 建立策略夥伴關係

我們在上面看到，SASE　架構直接向網際網路邊緣的設備提供安全服務，消除每次存取服務時必須與資料中心「保持聯絡」的浪費。但速度和延遲在雲端中仍然很重要：如果邊緣網路頻寬受限或與用戶設備的物理距離較遠，則延遲會增加並且性能會受到影響。

為了將這些限制降到最低，博通軟體事業部 (Broadcom Software) 在 Kubernetes 統合的容器化環境中重寫並重新構建其整個業務組合(80多種產品和服務，包括所有Symantec解決方案) 作為 Google Cloud 基礎架構上的軟體即服務解決方案。

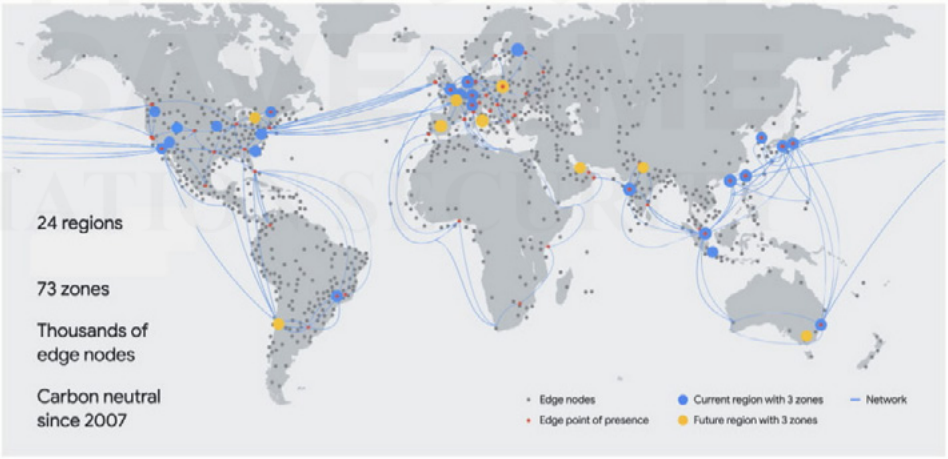
## 與 Google 建立策略夥伴關係 (續)

Google 現在為 Broadcom 和 Symantec 用戶提供以下優勢：

- **全球覆蓋率**，在高速專用網路上與 ISP、內容提供商和用戶互連
- 全球 180 多個網際網路交換和 160 多個互連的**邊緣設備存在點 (POP)**（參見下圖 1），降低了成本和延遲
- Google 專用骨幹網的**高效路由**，大量減少公共網際網路上的流量
- **無可比擬的規模**
- **彈性**回應不可預測的變化
- 面對服務中斷時的**穩定性**和韌性

雖然為期 18 個月的遷移，無疑對其客戶產生了影響，但現在賽門鐵克提供雲端解決方案績效卓越的安全性，並得到第三方的驗證。與公共網際網路相比，Google Cloud 上的 Symantec SASE 加密流量的吞吐量提高 144%，延遲降低 62%，未加密流量的吞吐量提高 14%，延遲降低 19%。賽門鐵克在總交易時間方面的優勢，隨著雙方之間的物理距離增加而益加明顯，同城市間的存取時間比公共網際網路縮短 21% ，比加州到新加坡間存取的時間縮短 62%。

**圖 1：Google Cloud定義的網路邊緣，2021 年 2 月**




來源：Google Cloud 部落格

Google Cloud 主幹網路讓 Broadcom 及其客戶受益：用戶上手速度更快，最新科技確保始終如一的高服務水準。賽門鐵克更與 Google 合作建立本地化區域--一種確保網路內容針對請求發出的國家／地區進行本地化的方法，即使 ISP 位於其境外也是如此。由於其全方位的雲端服務組合與對用戶所提供的優異效益，Broadcom 獲得 Google Cloud 2021 年度客戶獎。

## 產品線創新

任何情況下並不能被理解為在Broadcom收購賽門鐵克之後的這段時間內停止了產品創新。畢竟，作為一項政策，Broadcom 公司每年都會將其營收的 20% 以上再投資於研發。表 3 顯示賽門鐵克併入博通後推出的產品創新例子，包括在 Google Cloud 平臺整合時投入精力的高峰期。

**表 2：收購賽門鐵克後的創新實績**

| 賽門鐵克各產品線的創新 |
| --- |
| **端點安全** |
| • 調適型 (Adaptive) 防護系統統整來自不同地域、部門或其他實體的代理資訊，以應對當地情況，而不是全球共同標準。<br>• 新的儀錶板強化顯示高風險應用程式的異常行為，例如：PowerShell、Net.exc……等，以應對勒索軟體的「就地取材」和鎖定目標攻擊。<br>• 端點管理主控台移至雲端。<br>• 解決方案區域化，以解決資料主權和其他區域性問題。<br>• AD 威脅防禦 (TDAD) 保護目錄服務的完整性，透過混淆目錄，以對抗勒索軟體攻擊中典型的憑證竊取和橫向移動。<br>• 代理整合：單一代理，整合雲 SWG 所需的流量轉導向。 |
| **資料安全** |
| • 資料外洩防護方案的持續發展，從 15 版到 16 版，17 版即將推出。<br>• 基於使用以資訊為中心的分析的風險評分的新政策，建立在 UEBA (使用者與實體行為分析) 能力之上，且業務部門亦可使用。<br>• 統合各種事件，以方便管理。<br>• 使用 ServiceNow 整合組織的隔離，減少對監控的需求。<br>• 歐盟 GDPR 合規性創新，例如：允許管理員在不違反隱私法規的情況下，查看模糊化的事件日誌。<br>• CASB 現在支援透過雲端版本的 Enforce 管理 Oracle。<br>• CASB 為資料信任和傳輸中的資料 (Data in Motion)API、Securlet和閘道解決方案。 |
| **網路安全** |
| • 安全網路閘道(SWG)現在以虛擬機器或雲端服務的形式提供，其單一控制台適用於所有型式的 SWG。<br>• 多種網路功能現在可作為單一的SWG解決方案，包括雲SWG、邊際SWG、隔離、內容分析、SSL檢查、應用程式可視性和控制、智慧服務和集中管理與報告。<br>• 推出新開發的雲端防火牆服務，並讓所有 SWG 客戶可選用。<br>• 選擇性流量引導整合到安全網路閘道和 Symantec Enterprise Security Complete 的端點防護安全代理中。<br>• 基於代理和無代理的 ZTNA 現在是 VPN 的替代品，成本更低，安全問題更少，複雜性更低。 |
| **平臺和環境** |
| • 單一的 Symantec Enterprise Security Complete 代理整合安全網路閘道、零信任網路存取、CASB和端點功能。<br>• 向混合平臺邁進--而非純雲平臺，以因應大型跨國企業所需。<br>• 將使用者和實體行為分析 (UEBA) 從企業內部擴展到 CloudSOC CASB 和雲端 DLP。<br>• 引入 Mirror Gateway 技術，允許完全無人管理的設備，或無須任何代理程式，亦可安全存取企業網路。<br>• 擴增涵蓋 macOS 和 Linux 的 DLP 代理程式。<br>• 建立當地化語系區，針對請求的地理來源對網頁內容轉換為當地語系，而不考慮 ISP 的位置。 |

這些創新中的許多構成了跨企業內部、私有／混合和公共雲的技術整合或擴展。賽門鐵克的一個長期目標--賽門鐵克企業雲的單一代理和控制台--即將實現，並且已經存在雲中。公司還在朝著單一控制台的方向發展，將相當驚人地減少管理費用。

## 業務創新

正如賽門鐵克為改善其產品的可管理性而進行投資一樣，賽門鐵克更為企業客戶的利益而進行業務創新，以簡化和加速其自身的業務流程。現在，適用於數百個依功能、電腦環境、平臺等分類的貨號 (SKU) 亦已整併並簡化、並依使用者年份計價，提供客戶不受限制的使用安全類別的資源和資訊--端點、身份驗證、網路、資料等。過往企業客戶可能需與賽門鐵克簽訂二三十份合約--有各種各樣的條款和到期日--現在只需四份合約就能獲得賽門鐵克企業雲的完整保護。客戶可獲得以下好處：

- 在一個產品系列中獲得全方位的解決方案，實現無間斷的保護
- 提供有利於營運規劃的可預期年度成本結構，即使在使用量擴大的情況下也是如此
- 更低的整體網路安全成本
- 提供客戶更高的彈性，在沒有財務風險的情況下嘗試新的網路安全技術
- 簡化維護、升級和續約流程
- 致力於客戶服務秉持「協助客戶從解決方案中獲得最大利益」的理念
- 在一份合約中，不管是軟體、硬體、IaaS (基礎架構即服務) 上的虛擬或 SaaS (軟體即服務)，客戶可依自身各種因素自行選擇部署或重新部署所需安全功能。

這些定價計畫適用於大多數 Broadcom 軟體產品，為涵蓋網路安全、自動化、DevOps 和其他 Broadcom 技術的全公司簡化合約開闢了前景。

## 致力於志願協作社群與標準制定組織的貢獻

隨著監管和標準合規性在跨國公司決策過程中的影響甚鉅，對他們來說，擁有一個瞭解這些決策問題和可能業務影響的倡導者變得更加重要。多年來，賽門鐵克一直扮演著這樣的領袖角色，向美國政府、歐盟、聯合國和各種技術機構提供建議，宣導保護客戶的政策，而不給客戶的營運帶來非必要的負擔。以下是我們樹立的重要典範。

### 賽門鐵克致力於志願協作社群與標準制定組織的創新

- 賽門鐵克是網際網路工程任務組 (IETF：Internet Engineering Task Force) 和國際電信聯盟 (ITU：International Telecommunications Union) 中領先的網路安全廠商，國際電信聯盟是定義電信、資訊和通訊技術未來的聯合國團體。在過去的幾年裡，賽門鐵克為以下工作做出貢獻：
  - 參與國際通信聯盟 (International Telecommunication Union，ITU) 電信標準化部門 (Telecommunication Standardization Sector，ITU-T)的第17研究組--網路安全，負責制定全球網路安全標準。該公司最近借調一名賽門鐵克員工擔任該研究小組的副主席。
  - 博通賽門鐵克是開放網路安全模式框架(OpenCybersecuritySchemaFramework，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、各種可支援及加速採用 OCSF 模式的開源工具，賽門鐵克貢獻其綜合網路防禦模式，努力打破資料孤島，使網路安全解決方案之間的資料一致化，以加快資料分析，以協助組織更快也更有效率地偵測、調查與阻止網路攻擊。這篇部落文章和《富比士》這篇文章描述這項創新的意義。
  - 始終致力於推廣更安全的傳輸層安全標準 (Transport Layer Security--TLS) 1.3 的先鋒，該標準也代表其客戶需要檢查可能被隱藏在高階加密惡意軟體的流量。無疑的 TLS 1.3 對個人隱私提供更完全的保護，但對於企業安全則產生負面影響。這篇部落文概述這些問題。
  - 全面提供支援 ECH 加密協定的安全防護解決方案，ECH (Encrypted Client Hello) 是 TLS 的延伸，填補端到端傳輸層加密的最後空白。賽門鐵克發現一個問題--同樣與檢測有關--將其客戶置於監管風險之中，並積極確定解決方案。
  - 抵消網際網路標準「超區域化」的影響，出於法規和標準相互制約，成了越來越小的侷限性監管孤島，如果不進行合規性測試和可能的干預措施，就無法兩全其美。
- 在歐盟理事會主席國和歐洲議會確定《數位營運韌性法案》(Digital Operational Resilience Act，DORA) 時，就是因為賽門鐵克在布魯塞爾派駐代表並積極參與，所以賽門鐵克的產品被證實早在該法案生效之前就已經完全符合 DORA 的要求。
- 身為資料保護軟體的領導廠商，賽門鐵克參與歐盟資料保護委員會 (European Data Protection Board，EDPB)。我們最近發現法規的遵循與稽核過程中的一個風險，並透過在行政審查 (administrative review) 期間模糊化個人身份資訊的方式進行糾正。

## 未來創新週期

賽門鐵克不斷致力於安全框架和架構的創新，目的是減少管理和合規上的複雜性，以及東拼西湊式安全架構的顧此失彼和疊床架屋的諸多困擾。我們已經推出一個橫跨企業的解決方案，擴展 Gartner 的 SASE 框架，以加強對資料保護、法規遵循和威脅情報的關注。

### 賽門鐵克企業安全雲

賽門鐵克企業安全雲解決方案 (SEC) 是基於這些原則：

- **整合**：多種端點代理程式會消耗用戶端資源，增加複雜性，也徒增成本。SEC 的單一代理適用於所有端點：筆記型電腦、桌上型電腦、平板電腦、智慧型手機、伺服器和雲工作負載～終結散亂的代理程式，降低複雜性，並為管理人員提供所有端點的單一視圖。得力於可整合雲端安全網路閘道，該代理也為漫遊端點提供端點和網路安全。
- **混合雲**：許多企業由於業務、法律或監管方面的原因，必須保持企業資料中心架構：他們的雲端環境轉移將始終是一個混合雲環境。對於他們來說，賽門鐵克企業安全雲可以作為一個單一實體部署，跨越企業內部和雲端環境，對兩者進行統一管理。另外，它也可以作為一個 100% 的企業內部自建解決方案，在企業內部設立執行點，或者作為一個完全基於雲的實施方案，在雲中設立執行點。
- **資料防護和威脅防護在一起**：賽門鐵克企業安全雲將資料防洩露保護 (DLP) 與威脅防護結合起來，以保護穿越網路、閘道和端點的資料，識別並緩解攻擊。威脅檢測功能由賽門鐵克威脅獵手團隊和賽門鐵克全球情資網路提供，後者利用人工智慧可將超過9PB的資料轉化為精準行動的威脅情資。
- **整合SOC (Security Operation Center資訊安全維運中心)**：網路安全工具之間的整合使我們非常厲害的威脅獵手團隊能夠評估威脅資訊，察覺他人看不出來的模式，阻斷攻擊，並與客戶交流，以增強他們的 SOC 維運績效。
- **合規性**：賽門鐵克企業安全雲(SEC）適用於跨組織的持續性合規管理與控制。單一治理團隊可以從單一管理平台管理資料風險，並進行稽核。無論是在企業內部還是在雲端。
- **SSE**：對安全服務邊緣（SSE：Secure Service Edge）的支援是賽門鐵克的混合能力、以資料為中心的安全架構之一部分。

### 後續

接下來的幾年，隨著公司不斷將解決方案琢磨到更臻完美和執行其對賽門鐵克企業安全雲的願景，賽門鐵克的解決方案將彼此無縫接軌。客戶可以期待：

- 跨技術、平臺和環境的單一賽門鐵克代理～一個長期的網路安全目標，現在變得觸手可及了。
- 對整個企業環境中的合規性、確保遠端工作以及資料和威脅保護進行一致的管理。
- 在現有的授權合約下，可透過產品升級提供新功能。

## 後續(續)

統合是實現簡單、有效管理、持續一致的合規性、改善用戶體驗以及更有效地利用內部 (日誌) 和外部 (情資) 資料的關鍵。賽門鐵克企業安全雲提供所有這些，並以簡單、依用戶數計算的年度價格提供，涵蓋整個企業的端點安全、網路安全、資料安全和電子郵件安全解決方案。

**圖三：賽門鐵克企業安全雲**


## 結論

狹義的創新觀點片面關注新創企業的利基產品開發，並傾向於像今天的純雲解決方案這樣的趨勢。更廣義的觀點則考慮到公司的所有創新方式：透過收購、產業意見領袖的領導力、打造滿足客戶需求的解決方案，以及形塑商業和監管環境。

一路走來，賽門鐵克一直是引領所有這些形式的網路安全創新的的先鋒。身為博通的企業安全部門，賽門鐵克持續致力於客戶成功所需的解決方案、商業模式和志願協作社群等全方位創新。

**關於賽門鐵克**

賽門鐵克是資安業界的長青樹，品牌享譽至今超過四十年。賽門鐵克(Symantec)已於2019/11併入全球網通晶片巨擘--博通(BroadCom，美國股市代號AVGO，全世界網際網路流量有99.9%經過博通的網通晶片)軟體事業部的企業安全部門(SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通(Broadcom)是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec持續創新的技術能為日新月異的資安問題提供更好的解決方案，近年來Symantec很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦(CA Technologies)以及雲端運算及「硬體虛擬化」的領導廠商-VMware， 也是博通軟體事業部的成員)。2021年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署(CISA)宣布聯合民間科技公司，發展全國性聯合防禦計畫JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

**關於保安資訊**

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年起就全心全力於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，以及基於比原廠更孰悉用戶環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。