白皮書

自適應(Adaptive) 防護

可依狀態調整、隨機應變的創新防護技術，中斷複雜攻擊的關鍵能力

IDC 的觀點

終端設備 (端點) 已經並將繼續成為威脅發動者的主要覬覦對象。這些聯網裝置不僅是獲得高價值資訊資產的跳板，而且還是容易下手的目標。因為這些設備提供了多個管道的破口機會（網頁、電子郵件、實體媒體、軟體更新、遠程管理員連線和點對點應用程式）。此外，這些設備的終端使用者是人，只要是人就可以被操弄、被誘騙，並且應用程式及其配置和使用模式與每個終端使用者一樣獨特，並且可能會發生變化。工作標準也在不斷發展。投入到前所未有的大流行遠端工作實驗中，工作所在地點永遠變得更加虛擬和動態。此外，工作用的設備將越來越多地受到最終用戶偏好的影響，通常本著方便的精神。所有這些都為威脅發動者提供了廣泛的攻擊面和活動範圍，難以全面和確實地進行監視。

端點安全解決方案已經隨著高科技的防護和檢測技術的發展而提升，以降低這種始終存在的風險。然而歷史一再證明，惡意軟體仍然會攻擊終端使用者的裝置，威脅發動者進化他們的技術以逃避檢測（例如：利用系統管理工具或第三方管理工具的 living-off-the-land：就地取材的攻擊策略），並且鋪天蓋地的誤報困擾著安全分析師。因此，源自受感染端點的資安事件仍然居高不下。

IDC 的觀點是組織過度依賴端點安全中的保護和檢測機制，而忽略了強化安全形態和減少攻擊面的重要性。組織的端點安全技術與機制 / 彈藥庫應該更加全面性與均衡性。然而，旨在增強安全形態並減少企業規模的攻擊面、具有精確性和個性化，同時自動隨機應變不斷變化的環境的解決方案尚不存在。此外，對中斷業務運營和員工生產力的擔憂，增加了組織在為合法活動之外的所有活動定義和執行拒絕 / 黑名單方面的猶豫。

賽門鐵克最近推出的自適應保護通過限制威脅發動者的活動範圍來重新平衡企業的端點安全技術與機制。利用賽門鐵克關於受信任程序（例如：處理下載的合法可執行檔案）的行為的全球威脅情報，並結合人工智慧 (AI) 模仿和機器學習 (ML) 引擎，自適應保護自動生成程序行為的即時熱感圖和根據組織內行為的普遍性提供預防性建議（例如：拒絕或監控）。經由攔截 / 阻斷賽門鐵克已識別的特定行為，真正的攻擊政策會立即減少攻擊者的活動範圍，而不會影響日常流程。被先發制人破壞的是嘗試拒絕行為的攻擊鏈，只要任何鏈階被打破，攻擊活動就告失敗。

攻擊者始終會嘗試其他程序行為，其中一些行為已經發生在企業內部。自適應保護應對每個不同企業的獨特性來阻止這些攻擊嘗試。藉由深入研究即時熱感圖詳細內容，自適應保護管理員可以快速查看每個端點發生了哪些不常見的行為及其普及 / 普遍 / 發生頻率。有了這些知識，自適應保護管理員可以為單個設備、賽門鐵克自行匡列的設備，制定拒絕和監控規則，因為它們表現出類似的行為。

自適應保護也是動態的。隨著攻擊戰略和企業環境的不斷發展，自適應保護的熱感圖和建議經過精心設計能夠自動調整。攻擊技術和企業環境的變化帶來的風險變得更加可預防。

作為賽門鐵克端點安全的持續創新技術，自適應保護利用關閉企業端點內部和之間的異常行為的處理程序，降低了日益增加的端點被感染或成為跳板後衍生的一面倒的災難式骨牌效應後果。雖然，端點只是一種攻擊媒介，惡意行為的處理程序也只是風險的一種指標。 但營運優先、便利性以及效率化本質和威脅發動者持續進化的隱蔽操縱端點的能力相結合，促成了網站、電子郵件、訊息和檔案共享應用的大受歡迎，而這些常用的共享應用常被利用於向端點傳遞惡意程式並誘使終端用戶洩露敏感資料以及更嚴重的大規模攻擊及更嚴重的資安災難。

所有應用程式都有其不同的處理程序行為 (process behaviors)，例如：網頁存取、點對點通訊和檔案分享等是常見的應用，而且情況各不相同，也時常在改變。正當合法性可以瞬間改變，不能以表層價值來假設。廣泛收集並詳細解讀最新的威脅情報，

對於自適應評估風險和執行針對每個企業員工的網路、通訊和檔案共享活動量身定制的降低風險規則至關重要。有利的是，賽門鐵克已經領先一步，已用於端點預防異常處理程序行為的自適應技術，將擴展到完整的保護方案。

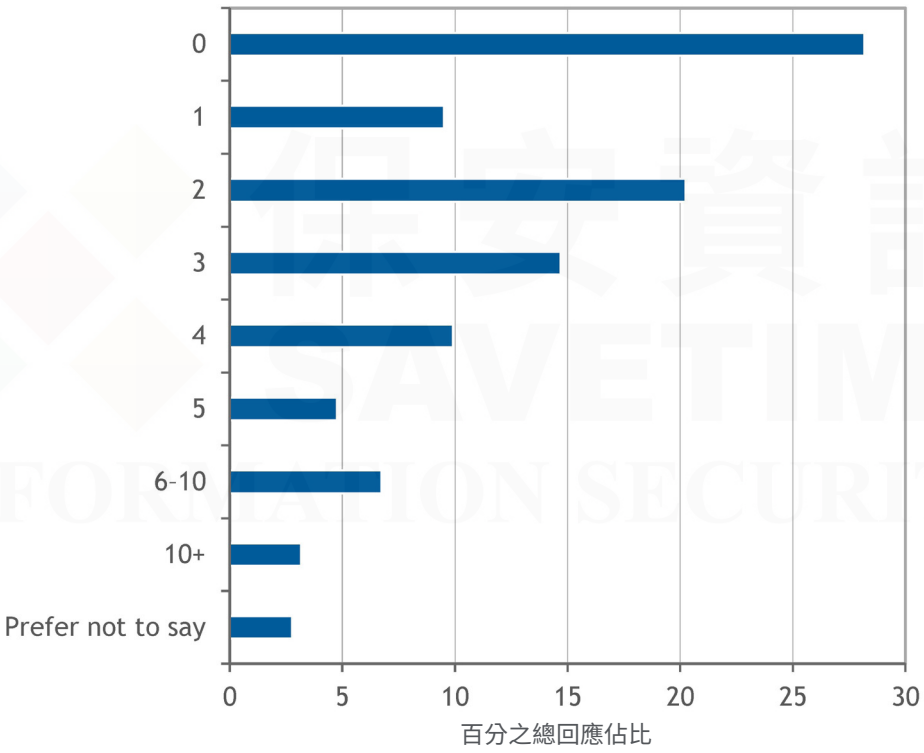
保護和檢測技術還不夠

對於許多組織而言，當前的網路安全解決方案和手法未能完全實現其降低風險的目標。在最近的 IDC 調查中，擁有 5,000 多名員工的受訪組織中有 60% 每年至少遭受一次重大安全漏洞。只有不到三分之一的受訪組織聲稱在過去兩年中避免了重大的資安危害（見圖 1）。

圖 1

過去兩年的重大安全漏洞

Q. 在過去兩年中，您的組織大約有多少重大資安危害事件需要花費大量額外資源來修復？



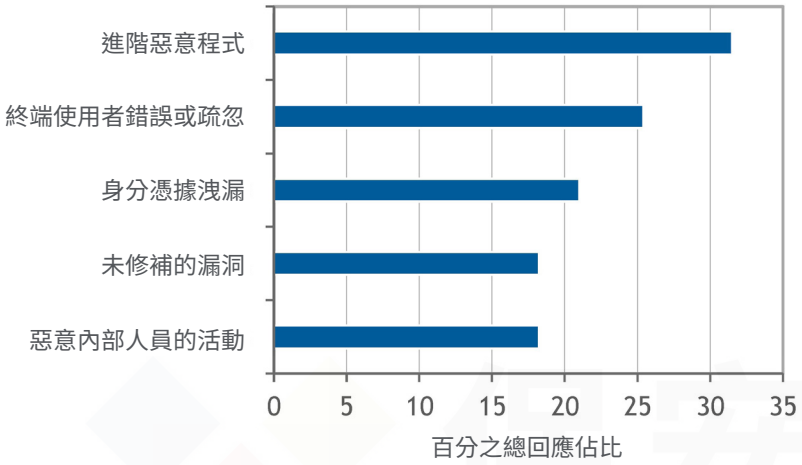
n = 252 (組織員工大於 5,000 人的單位)
資料來源：IDC 2020/12，關於 EDR 及 XDR 的調查

儘管絕大多數組織使用端點安全產品，也有一些組織使用多品牌供應商的產品，但進階惡意程式還是資安危害事件的常見原因，其次是終端使用者錯誤或疏忽和身分憑據洩漏（參見圖 2）。

圖 2

最常見的資安危害事件的原因

Q. 以下哪些是最常見的資安危害事件的原因？從 12 個表列原因中依比重，最多選擇 3 個。）



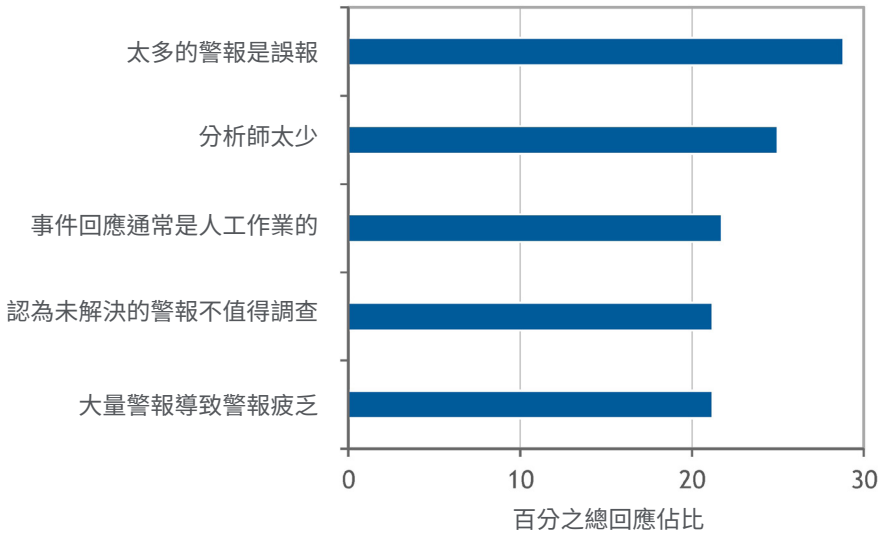
n = 181 (組織員工大於 5,000 人的單位)
資料來源：IDC 2020/12
關於 EDR 及 XDR 的調查

正如 IDC 的調查所證實的那樣，資安危害事件的數量與未調查警報的數量以及調查警報所用的時間之間也存在正相關關係。此外，導致未調查警報和調查時間的因素是誤報警報（即正常的判斷為有問題需調查的）和警報疲乏（見圖 3）的數量。

圖 3

影響組織調查和回應可疑警報的原因

Q. 是什麼原因影響您的組織每週調查和回應所有可疑警報？（從九個列表中，最多選擇兩個原因--顯示的前 5 個原因。）



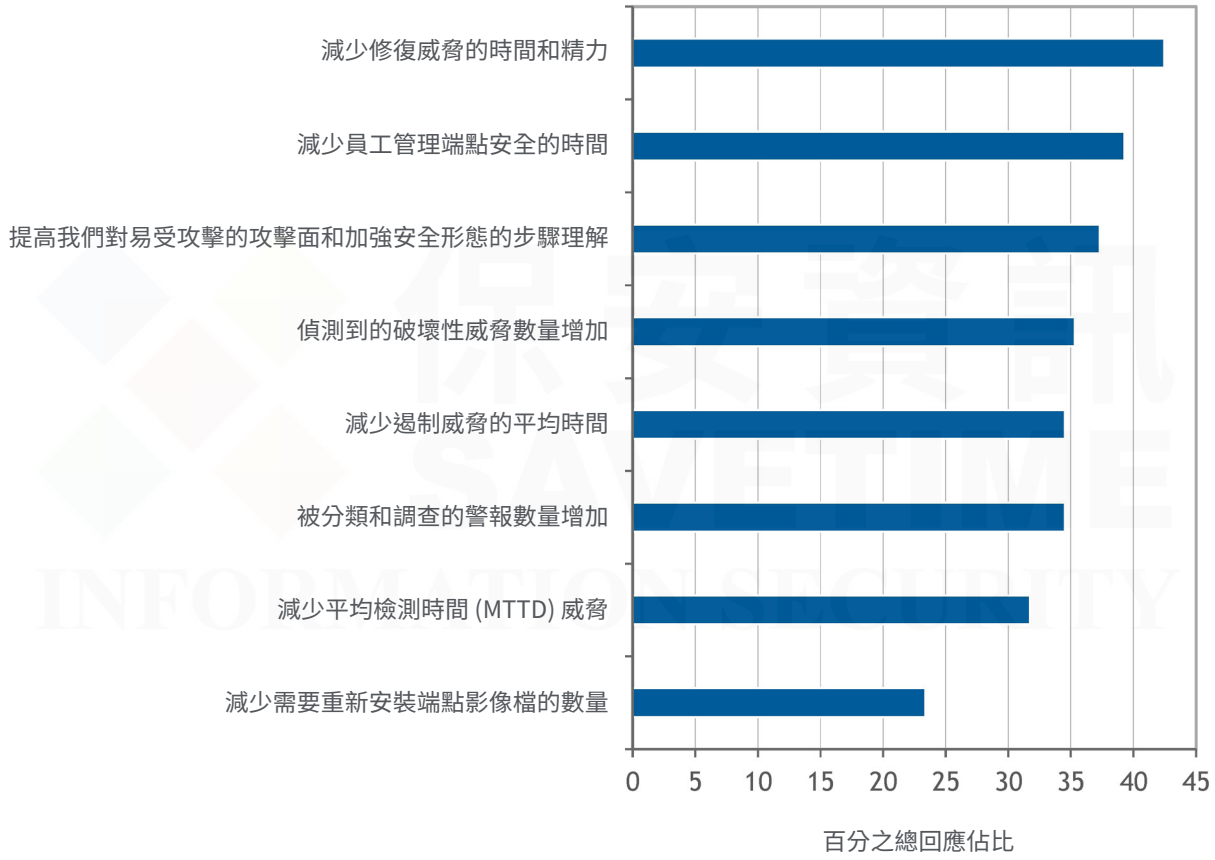
n = 184 (組織員工大於 5,000 人的單位)
資料來源：IDC 2020/12
關於 EDR 及 XDR 的調查

隨著組織轉向端點偵測與回應 (EDR) 來改進他們的防禦，他們的報表，真的顯示出許多具體的效益（參見圖 4）。然而，並非所有效益，都是 EDR 的偵測與回應的重要核心任務。了解有破口的攻擊面並深入了解加強安全形態是最常提到的好處之一。儘管有益，但這種理解是在威脅發動者已經滲透到組織環境之後發生的。儘管如此，這種 EDR 的優勢更證明了預防並減少其被攻擊面和強化安全形態的價值。

圖 4

EDR（端點偵測與回應）所提供的效益

Q. 以下哪些是 EDR 為您的組織帶來的最重要的好處？（從列出的八項中最多選擇四項。）



n = 252 (組織員工大於 5,000 人的單位)
資料來源：IDC 2020/12，關於 EDR 及 XDR 的調查

EDR 並不是聚焦易受攻擊面的唯一方法。定期的藍隊和紅隊練習和滲透測試也增加了理解。然而，這些方法有其局限性：

- **亡羊補牢的解決方案定位**：對試圖利用當前漏洞的當前威脅進行的練習和測試，是對阻止下一次攻擊技術的準備情況的不完整評估，或衡量歸因於企業環境未來變化的漏洞。這將不得不等到下一次預定的評估。
- **所需的專業知識**：經驗和人才是必不可少的，但許多組織沒有足夠的裝備或資金來進行適合其企業情況的練習和測試。
- **不是封閉迴路系統**：演練和測試可識別安全落差和漏洞，並可能會建議改進安全形態的步驟。不幸的是，這些建議可能過於複雜和耗時，無法快速實施，從而使企業經常處於高風險的安全形態。

自適應防護技術，對扭轉對手至關重要

深入審視現有資訊安全的實施方式，會發現威脅發動者是有足夠的空間來操縱並取得成功。無論是端點安全、入侵偵測、郵件或訊息內容過濾還是網頁安全，都旨在高度自信地阻止可立即識別為惡意或不需要的威脅。無論支持自動檢測和阻止的機制使用哈希、簽名、聲譽、類別、行為分析、ML/AI，還是某種組合，都是如此。

雖然自動化檢測的進步擴大了識別和阻止的威脅範圍，但經驗豐富的威脅發動者會精進他們的攻擊技術來躲避檢測。正如 IDC 的調查所指出的那樣，進階惡意程式是被最常被利用的武器。

經驗豐富的威脅發動者還會就安全產品的運行方式進行自我教育。通過對這些產品進行逆向工程、進行偵察和反覆試驗，他們磨練了逃避自動檢測的能力。

然而，有理由繼續使用通用的、一體適用的安全產品。從業務角度來看，在不影響正常業務流程（即業務透明度）或增加安全人員工作負擔的情況下，可以阻止廣泛類別的攻擊類型。

此外，安全團隊可以選擇定義和強制執行自定義阻擋 / 封鎖規則集以阻止特定活動。然而，這種補充方法有缺點。首先，平衡安全風險和業務透明度仍然是一個考慮因素，更多、更精細定義的規則，使這種平衡行為更具挑戰性。其次，生命週期規則集管理是必要的，並且通常是手動操作，因此本質上不具有可擴展性。第三，威脅格局的變化會降低規則集的效力，不可避免地，持續存在的威脅發動者將尋求規避定制規則。

面對一體適用的通用型安全產品和自定義規則集的局限性，加上威脅發動者的不斷推進，組織已經提升了他們被入侵後的偵測和回應能力--一個審慎的亡羊補牢安全層，但也是一個被動的核心層。若要取得成功，必須在組織的 IT 環境中偵測到威脅發動者的行為，並在損害發生之前加速全面性的威脅遏止。在最好的情況下，遏止也應該是業務透明的。考慮到組織 IT 環境不斷擴展和變革的狀態，威脅發動者有更多的新空間來操縱，這使得偵測和回應的挑戰越來越大。

IDC 認為，要扭轉威脅發動者的局勢，預防需要成為安全實作的核心。當然，預防的整體概念並非新鮮玩意，它一直是一個長期存在的基礎元素。然而，在今天的情況下，預防並沒有像過去那樣有效。為了在當今的超動態的威脅格局和 IT 環境中變得更加有效，IDC 認為應該針對以下屬性優化預防：

- **自適應能力**：隨著威脅格局和 IT 環境的變化，預防機制也必須具備隨機應變的的適應以保留並更好地提高其在縮小威脅參與者進入、感染和攻擊或破壞力方面的效力。
- **可客製化**：每個組織的 IT 環境、安全防護技術和風險承受能力的組合都是獨一無二的。因此，必須為每個組織量身定制預防措施。
- **自動化**：威脅發動者剛開始是利用安全防禦中的漏洞而取得入侵的機會，之後，再來展開更周全的攻擊。為了優化預防的有效性，必須通過自動化來促進自適應和客製化，讓威脅發動者無機可趁，同樣重要的是，可大幅減少對安全人員的時間和心力的需求。
- **可擴展**：由於威脅發動者利用多個入站和出站媒介，組織採用了多種形式的安全技術。自適應和可客製化的預防應該是可擴展的，盡可能擴充至多重安全技術。
- **業務透明**：預防的有效性需要即時運作，這需要在業務流程中運作。因此，為了不阻礙流程，必須在開始執行之前以高準確性和全面的方式評估預防的潛在不利影響，並在此後持續監控以預先評估未來可能的影響。

針對這些屬性進行優化，預防可以帶來以下額外好處：

- **增加威脅發動者的成本**：通過自適應和可自訂化，每個組織的安全防禦機制都不同。因此，威脅發動者用來規避標準安全配置的可重複操作手冊和技術不太可能成功。為了克服這一點，威脅參與者需要將他們的攻擊方法從自動化和可重複的技術升級為專為單個目標設計的定制技術。攻擊者喜歡的一對多回報效益將不再可行，這可能會說服攻擊者將其資源用於其他防禦較差的目標。
- **降低偵測和回應工作量**：通過預防減少攻擊者使用的途徑，良性和嚴重警報的數量有望減少，安全事件也是如此。在事件數量驅動的操作中，安全團隊可以看到他們的反應性、偵測和回應的工作量減少，使他們能夠專注於更少的事件，並可能將他們的精力重新分配到具有戰略重要性的安全計劃上。

解決方案

作為賽門鐵克的第一個自適應解決方案，自適應保護基於限制攻擊者在受感染端點內外的活動範圍，來減少企業的攻擊面，並增強企業的安全形態。自適應保護是建構在賽門鐵克的全球威脅情報、人工智慧模型和機器學習引擎的基礎之上。同時，它們會自動建立和更新用於攻擊的可信任程序行為的即時資料庫，並提供企業流程和行為的全面可見性。結合更多先進技術，包含賽門鐵克提供了有關這些涉及受信任程序行為的真實情境的普及情況熱圖。

對於企業內部從來沒有發生過的行為，這是一個低風險的拒絕決定。如果以後發生這些行為，它們將被自動阻止。換句話說，不常見的行為與同一可信任程序相關聯的其他行為隔離開來並分開處理。

通過對行為頻率和所涉及的端點設備進行排名，進一步採取自適應保護，安全管理員可以針對單個設備、按組織分組的設備（例如：財務、人力資源、IT 或營銷）的每個行為啟用拒絕、監控和允許政策，或基於行為共通性的賽門鐵克所分類的設備群組。這種精闢的理解還可以幫助安全管理員優先調查涉及可信任程序行為的正當合法性。

鼓勵安全管理員進行調查並增加拒絕強制執行是自適應保護在其安全防禦中產生的自定義。他們在安全防禦中越強調獨特性，相對於不那麼獨特的組織而言，他們的組織作為目標的吸引力就越小。此外，他們的端點設備的安全形態將獲得強化，因為被拒絕的行為不再代表安全風險，因為它們被阻止發生。

自適應保護還引入了快速調諧設置。Quick Tune 可識別所有不常見行為（即環境中不存在的行為）並將其配置為拒絕。這極大地簡化了管理員的工作流程，只需要管理員的批准即可使這些設置在產品中生效。Quick Tune 進一步縮短了實現價值的時間，並簡化了自適應保護的採用。

機會

IDC 認為，當賽門鐵克將自適應防護的依狀態調整和客製化功能擴展到其他賽門鐵克安全技術和平台時，賽門鐵克自適應保護的市場機會將進一步加強。

從自適應保護開始是賽門鐵克自適應保護功能的合乎邏輯的第一步。正如我們之前所說，最終用戶及其設備經常成為攻擊目標。因此，端點安全被廣泛接受為網路安全的關鍵第一道防線。

隨著 COVID-19 大流行，終端安全的這種重要性變得更加突出，因為大量訊息工作者突然被迫全職在家工作。與此同時，組織加速了向雲端服務的遷移。IT 環境中的這種分散性，雖然在大流行封鎖期間必不可少，並且也與組織的戰略數位轉型計劃保持一致，但使端點更具針對性，因為它們在企業網路防禦保護之外運行，最終用戶獲得更多且頻繁的直接網際網路存取雲端資源。遠程工作和雲端使用都不會恢復到大流行前的水平，因此有效端點安全的重要性不會減弱。

自適應保護也非常符合零信任的概念。隨著安全管理員在使用自適應保護方面取得進展，受信任程序所允許的行為將越來越僅限於組織環境中常用的行為，禁止所有其他行為。

對於努力在零信任方面取得切實進展的安全團隊，自適應保護提供了一種實用的方法。IDC 預計，隨著賽門鐵克將自適應保護的功能擴展到其他賽門鐵克安全平台，與零信任的一致性將繼續，為安全團隊提供統一的方法來更廣泛地實施零信任。

今天通過端點保護平台、端點檢測和響應實踐的端點安全，仍然高度依賴於了解威脅發動者的運作方式，嘗試預測他們的運作方式，以及全面、快速地檢測和響應危害。雖然在多層防禦中必不可少，但自適應保護提供了一種互補、強大且業務透明的方法，用於減少端點的攻擊面、加強安全形態並限制威脅發動者的活動範圍，包括橫向移動。正如我們之前所說，自適應保護可以對事件應變人員降低工作負擔帶來正面助益。

最後，大型企業長期以來一直是新安全技術的先行者。然而，隨著時間的推移，他們來自多個供應商的安全技術堆疊變得過於廣泛和複雜，無法提供所需的安全結果。所需的補救措施是減少安全供應商的數量，同時獲得更緊密的跨產品整合和整體可管理性。他們還需要證明他們的戰略安全供應商將持續創新，以對抗隨著時間的推移變得更加複雜、有針對性和殘酷無情的威脅形勢。賽門鐵克內部開發的自適應產品線計劃表明賽門鐵克正在繼續創新之路。

挑戰

我們認為賽門鐵克將面臨的主要挑戰是贏得持懷疑態度的買家群體。受到其他替代或附加安全技術的影響，這些技術無法實現降低風險或操作簡便性的期待，現有供應商或新供應商都不會輕易擁有這些技術。將需要更大程度的預先展示價值，尤其是易

用性。Symantec Endpoint Security Complete(SESC) 代理中包含自適應保護，這對賽門鐵克有利。由於無需部署額外的代理程式，與現有 SESC 客戶進行廣泛的概念驗證應該是可行的。安全價值的第一次實例化顯示在受信任應用程序之間行為的熱圖可見性中，可能使客戶能夠量化他們以前無法評估的風險方面，這也應該對賽門鐵克有利。

結論

在資安的攻防上，威脅發動者輕而易舉就能佔據上風。隨著 IT 環境不斷擴大和遠端分散化，他們只需要找到一個未受保護或保護不足的入口點。從最初的感染開始，它們很容易向外擴展到其他設備和系統。威脅發動者一直在尋找掩飾其惡意行動的方法，轉而劫持受信任的程序，因為他們不太可能受到約束，以免影響合法的業務運營。

Symantec Adaptive Protection 提供了一種防止威脅發動者 (壞蛋)，濫用受信任程序暗度陳倉的新方法。結合對異常行為的瞭若指掌以及能夠仔細檢視所有已發生行為和流程 (即可視性)，安全管理員能夠自信地對合法流程進行限制，而不會限制業務。此外，Adaptive Protection 產生的可客製化措施，使每個環境都得到獨特的保護，較不易受到攻擊者標準化和可重複戰略的影響。從 IDC 的角度來看，自適應 (Adaptive) 防護是一項長久以來望眼欲穿的創新技術，值得添加到組織的端點安全武器庫中。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。
若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或
賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY
保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw