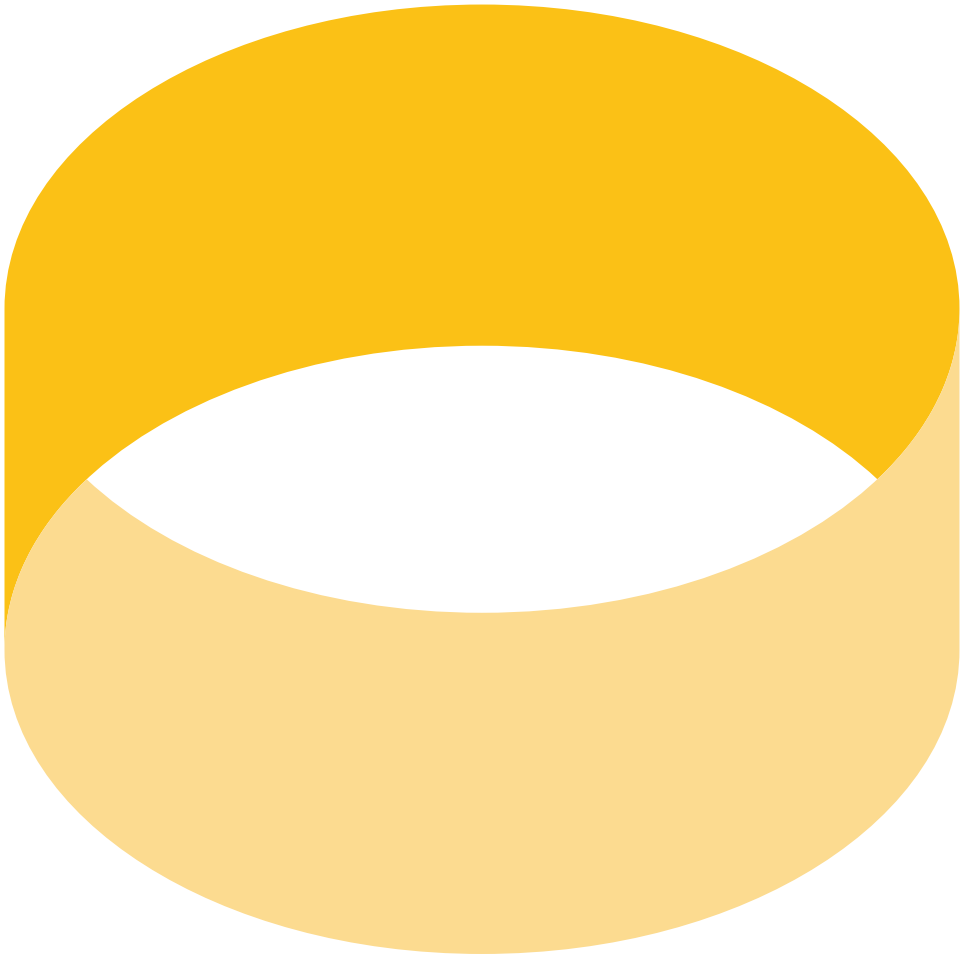


# 以 Symantec Endpoint Protection 達到零時差防護

## 套用零信任模型，搭配應用程式隔離功能與防惡意軟體

白皮書

Symantec™

2017 年 10 月 25 日

**聲明**

此文件由賽門鐵克 (Symantec) 統籌之後發佈，並接受下列企業的支援或間接合作而成：

**作者**：Sheetal Venkatesh、Ashok Banerjee、Torry Campbell

**撰寫人**：Deb Banerjee、Susan Hassall、Balaji Prasad

# 目錄

**只要交給防惡意軟體與應用程式隔離功能，可達 1+1 = 3 的效果** **3**

**為何受信任的應用程式反而風險最高** **3**

**避免來自於善意應用程式的攻擊** **3**

**強勢整合列入黑名單、列入白名單、應用程式隔離等功能** **4**

**案例研討 – 實際運作的「Jail」與「Castle」模式** **6**

案例研討 1：使用應用程式隔離功能的「Jail」模式，預防可發動攻擊的系統公用程式 **6**

案例研討 2：透過應用程式隔離功能的「Castle」模式，預防以 MS Excel 發動的無檔案攻擊 **7**

# 只要交給防惡意軟體與應用程式隔離功能，可達 1+1 = 3 的效果

逐漸分層的防禦方式，迫使攻擊者必須改採無檔案的「自給自足」攻擊技巧，且難以用傳統方法偵測得知。越來越多攻擊者更嘗試利用裝置上的現有資源，來達到自己的目標。現在根本不下載任何新的可執行檔或檔案，因此檔案式的偵測方式已逐漸失效。攻擊者不斷刺探常見應用程式的漏洞，並使用文件檔案中的指令碼內容，在受信任的應用程式背後偽裝自己的活動。他們也在記憶體中直接發動攻擊、隱身於登錄機碼中，並使用如 Powershell、WMI、Javascript、WScript 等常見的指令語言，避免引起懷疑。

為了防禦這類新的「自給自足」的戰術，賽門鐵克現整合了應用程式隔離功能與防惡意軟體成為單一解決方案，阻絕越來越多的零時差威脅。在防惡意軟體偵測並避免惡意軟體執行之時，應用程式隔離則假設惡意軟體能夠規避偵測，並已於您的端點上執行。當整合兩者之後，應用程式隔離則能強化防惡意軟體的優點，主動封鎖任何應用程式正使用零信任模型 (zero-trust model) 的可疑行為，不論是已知或可疑的應用程式皆然。

本篇白皮書將為您解釋：該如何使用這些由 Symantec Endpoint Protection 所提供的互補應用程式隔離與防惡意軟體功能，達到更全面的分層安全方式，且不致影響既有的產能。

# 為何受信任的應用程式反而風險最高

有許多應用程式攸關您的產能和每日營運狀況。這些應用程式包含了瀏覽器、電子郵件用戶端、生產力應用程式 (Microsoft Office)、平台工具 (Java)、常見開發工具 (Visual Studio)，以及其他更多應用程式。

大多數的應用程式都有漏洞，而且易於遭攻擊者刺探之後控制該應用程式，在您的端點中找到立足點，最後就是整個網路淪陷。如 Microsoft Word、Excel、Adobe PDF 檔案等的文件亦允許指令碼內容；這代表攻擊者能從看似無害的文件中執行惡意程式碼。而這類應用程式也需要較高權限才能正常運作，特別是需要管理權限使用者情境中執行的應用程式。因此，當攻擊者控制這些應用程式之後，就能無限制地存取端點。攻擊者可透過已入侵的應用程式下載惡意軟體酬載，再於受信任的應用程式情境中執行。

只要修正應用程式並升級至最新版本，是可以減少部分的問題。但在大型環境中，要隨時修正或更新有其難度。此外，零時差漏洞不斷增加，即便確實定期更新軟體也往往難以追上修補腳步。因此，我們必須採用防禦性的方式來阻絕對應用程式的刺探或竄改，進而避免攻擊者透過應用程式漏洞來感染整個環境。

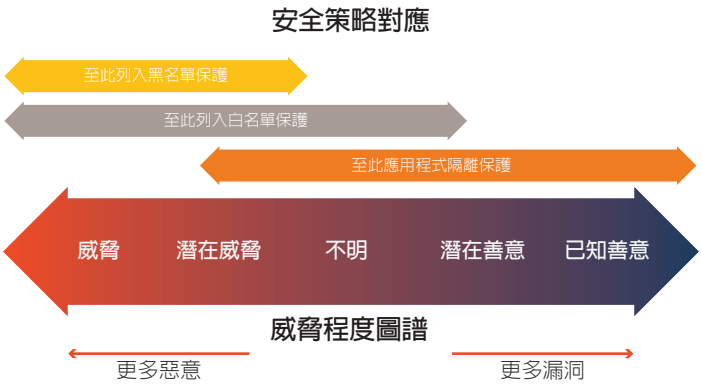
# 避免來自於善意應用程式的攻擊

此威脅程度圖譜，為您有效分析不同威脅媒介的正確防護策略。如果要分類某一端點上的所有檔案與應用程式，大抵可分為 5 大區塊：「威脅」、「潛在威脅」、「未知」、「潛在善意」、「已知善意」。


圖 1. 威脅程度圖譜。

有效的端點安全策略，往往是對完整的威脅程度圖譜提供防護。已知的惡意應用程式，即所謂的「威脅」，當然應立刻封鎖並消滅之。另應監控「潛在威脅」和「未知」的應用程式直到確認為止，接著在其傷害作業系統或其他應用程式之前阻擋行為。「潛在善意」和「已知善意」應用程式則予以保護，避免受到刺探而進行無檔案攻擊。

若要落實此一策略，就需要能整合多重控制功能的解決方案：




1. **列入黑名單 (Blacklisting) -** 根據預設的許可模型運作，讓所有應用程式自由執行，但已歸類為「惡意」的應用程式除外。這種模型將列舉已知惡意的應用程式、程序、指令碼等等，並在找出它們之時立刻消滅之。如果應用程式尚未分類為「惡意」，則將假設為「無害」並允許其執行。對於像是一般使用者常更換的桌上型和筆記型電腦等端點來說，這種安全模式易於部署且具備簡單有效的政策，因此為最受青睞。對於消滅已知威脅也頗有效率，但對於已遭侵入並正執行惡意行動的已知應用程式，就無法有效防護。
2. **列入白名單 (Whitelisting) -** 根據預設的拒絕模型運作，僅允許執行白名單 (各應用程式各有其政策) 之內的應用程式。除此之外，完全不信任或允許任何應用程式，因此可有效降低整體攻擊層面。不常變更的環境可順利運作此模型。但若能妥善管理此模型，則同樣可用於常常變化的「潛在威脅」。另外，只要零時差威脅跑出允許的行為之外，列入白名單模式也能找出並避免之。只要是列為白名單的應用程式，即便執行威脅活動也不會受到制止。
3. **應用程式隔離 -** 根據零信任模型運作，並以白名單安全為基礎，會允許已核准的應用程式，也會限制已核准應用程式的行為。舉例來說，某一應用程式的隔離政策，可用以定義該應用程式可接受的網路連線、檔案活動、登錄活動等，但也受限已知的善意行為。未列入白名單的應用程式雖可執行，但會受到極嚴苛的限制。因此，此模型可有效降低整體的攻擊層面。同時也能限制已許可的應用程式進行惡意作業，如變更受保護系統的設定或應用程式，進而減少零時差攻擊。

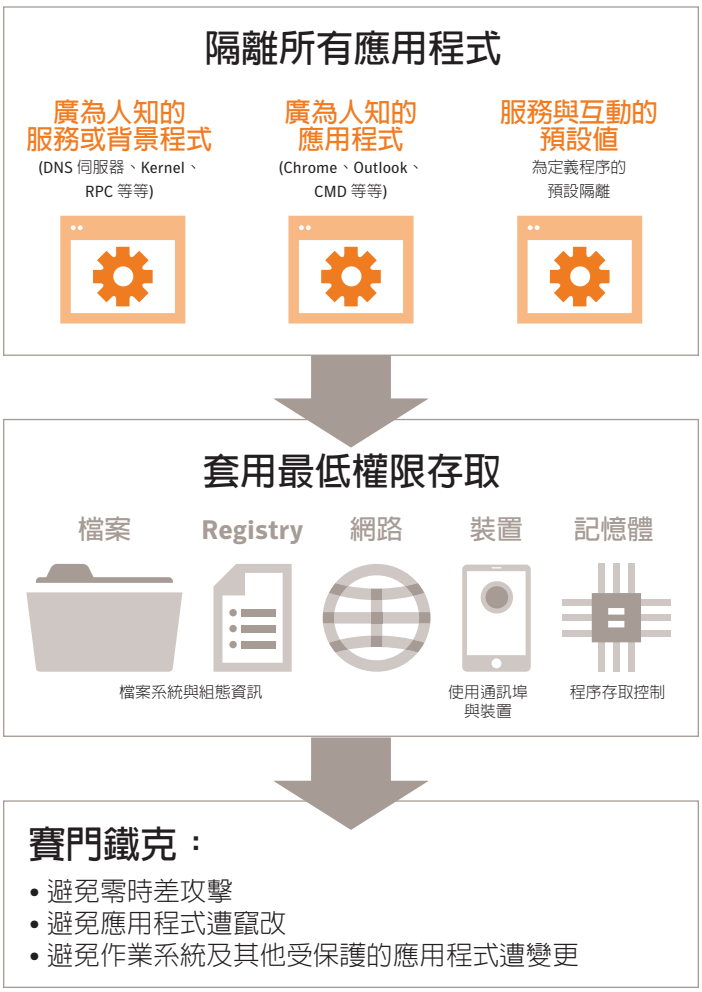



圖 2. 包含應用程式隔離的零信任 (Zero Trust) 模型。

# 強勢整合列入黑名單、列入白名單、應用程式隔離等功能

賽門鐵克為業界首次整合了黑名單、白名當、應用程式隔離等安全模型，將提供全方位的多層次防護功能，為您的端點阻絕威脅不受傷害。直到現在，這些可互補的技術仍用於保護非重複的端點。在統合了這些安全模型之後，幾乎達到了最大的防護範圍，更讓多樣的攻擊媒介均束手無策。


圖 3. 集結了防惡意軟體引擎的 SEP 所提供之分層防禦策略。

針對端點防護，Symantec Endpoint Protection (SEP) 另提供必要的多層式控制。在整合了防惡意軟體、裝置控制、減少攻擊、進階機器學習，以及行為監控引擎之後，SEP 可說達到了業界最佳的威脅防護效率。因此，SEP 可讓您找出已知的威脅和活動，即便只是初步懷疑也同樣能進行適當防禦。

SEP 的新「密集防護」功能，讓你僅需一個按鈕就能調整威脅偵測引擎，以封鎖所有的「威脅」並偵測「潛在威脅」。只要是已認定為威脅的檔案，密集防護功能將刪除或隔離該檔案，避免其繼續造成傷害。

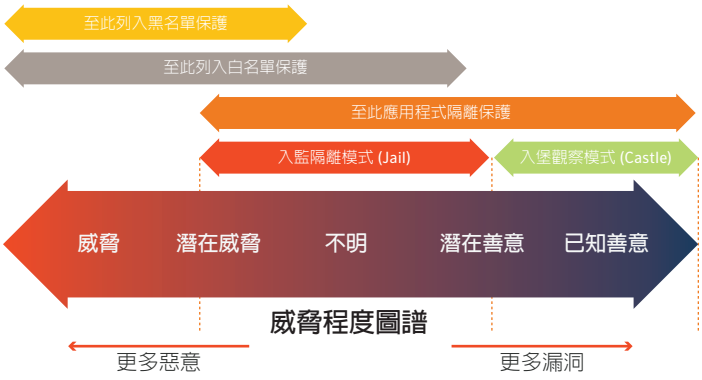



圖 4. 完整囊括威脅程度圖譜。

針對「潛在威脅」或「未知」的應用程式，密集防護將標記該檔案為可疑檔案，並交由附加元件產品 Symantec Endpoint Protection Hardening 的重要功能「應用程式隔離」處理。

應用程式隔離將以「入間隔離」(Jail) 模式執行這些可疑應用程式，使其在如監獄的環境中執行。應用程式將以受限的權限執行，以保護作業系統及其他善意應用程式，避免遭到竄改或傷害。其中也包含了從未受信任來源 (如網路或電子郵件) 開啟的項目，藉以降低風險並限制應用程式僅能執行「善意」行為。同樣的方式亦可套用到「潛在善意」的應用程式上；即一般不會執行可疑行為，但也未具備可信任信譽的應用程式，因此無法完全信賴之。應用程式隔離功能可於「電子腳鐐」類型的監獄中執行這類應用程式。帶上了「電子腳鐐」之後，應用程式的行為將大幅受限，如修改作業系統或安裝新應用程式等的權限作業均將禁止。

應用程式隔離功能，亦可保護「已知善意」(即列入白名單) 的應用程式，並以「入堡觀察」(Castle) 模式保護受信任的應用程式，另透過多層式安全保護其遭到刺探或竄改。首先，SEP 的「降低記憶體攻擊風險」(Memory Exploit Mitigation) 引擎，將保護應用程式的程序，避免受到多樣的刺探攻擊技術襲擊已知與未知漏洞。接著針對極端活動 (如攻擊者企圖控制應用程式的程序)，攻擊者將無法透過其程序權限安裝新軟體、變更系統設定，甚或修改其他應用程式的程序或資源。只要是應用程式在一般情況下不需執行的所有作業，均將由隔離政策封鎖。另必須說明的是，除非應用程式確實進行惡意行為，否則一般使用者在使用應用程式期間均不會察覺到任何變化。這也是高效率應用程式隔離功能所必備的特性，才不致影響整體產能。

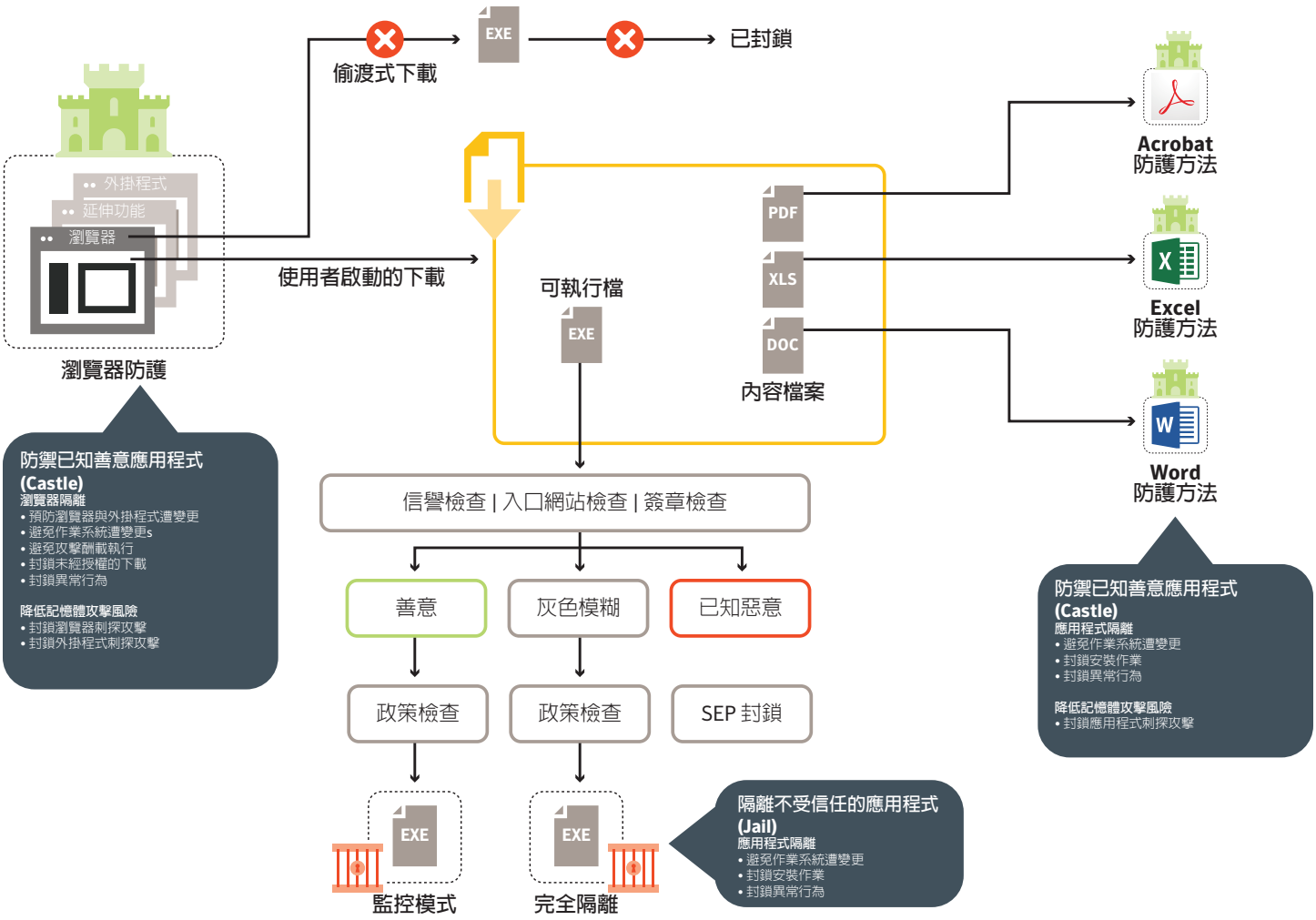



圖 5.「Jail」和「Castle」的運作方式。

在整合了列入黑名單、列入白名單、應用程式隔離等強大控制功能之後，即使攻擊者突破了密集防護的堅實屏障，也會遭到隔離並無法擴散，讓攻擊行為徒勞無功。

## 簡單易用

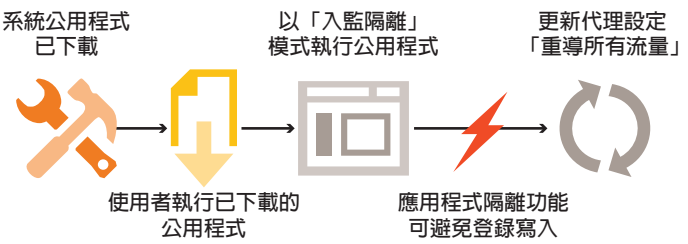
安全效率甚至重要，而且並不會影響整體產能。SEP Hardening 使用專屬的應用程式隔離技術，僅會對端點的效能產生最小影響，且並無其他特殊的硬體需求。除非應用程式確實進行可疑行為，否則一般使用者往往不知道應用程式隔離功能正運作中。另由於 SEP Hardening 可存取應用程式，並僅對可疑應用程式施行「Jail」模式，因此資安團隊亦可大幅減少處理誤報的時間。簡單易用的 SEP Hardening 僅對效能與產能造成最小的影響。

# 案例研討 – 實際運作的「Jail」與「Castle」模式

## 案例研討 1：使用應用程式隔離功能的「Jail」模式，預防可發動攻擊的系統公用程式

**問題：**一般使用者珍妮想透過公用程式「加快」筆記型電腦的效能。她造訪了知名的程式下載網站，挑了幾款公用程式並下載了「SpeedUp.exe」應用程式。珍顯然不知道「SpeedUp.exe」其實暗藏禍心，會修改 Windows 的代理設定並將網路流量導向攻擊者的伺服器。

**解決方案**：應用程式隔離功能將抵禦此威脅，避免攻擊者在端點取得立足點。




**運作方式**：在下載了「SpeedUp.exe」之後，Symantec Endpoint Protection 隨即徹底分析該檔案。密集防護引擎則判定「SpeedUp.exe」為可疑應用程式 (潛在威脅)，但尚未確認其為惡意軟體。因此，在使用者開啟「SpeedUp.exe」應用程式時，應用程式隔離功能隨即自動以「入監隔離」模式執行之。以入監隔離模式執行的「SpeedUp.exe」，只要未企圖讀取或修改任何受保護的作業系統資源，仍可安裝自己的使用者介面並檢查系統效能。一旦該應用程式企圖存取系統登錄檔，修改 Windows 的代理設定，隨即就會遭入監隔離模式封鎖作業並產生安全事件。此時系統將告知珍已封鎖了「SpeedUp.exe」修改作業系統，但仍能繼續執行其系統效能的公用程式。另必須一提，亦可設定 SEP 防止任何可執行檔從網路下載檔案。在此範例中，我們仍允許下載所有檔案，藉此展示「入監隔離」模式處理威脅的方式。

**優點**：應用程式隔離可動態地讓可疑應用程式「入監隔離」，避免端點遭到惡意修改。珍可繼續工作，不需顧慮其電腦或所連的網路是否遭受風險。

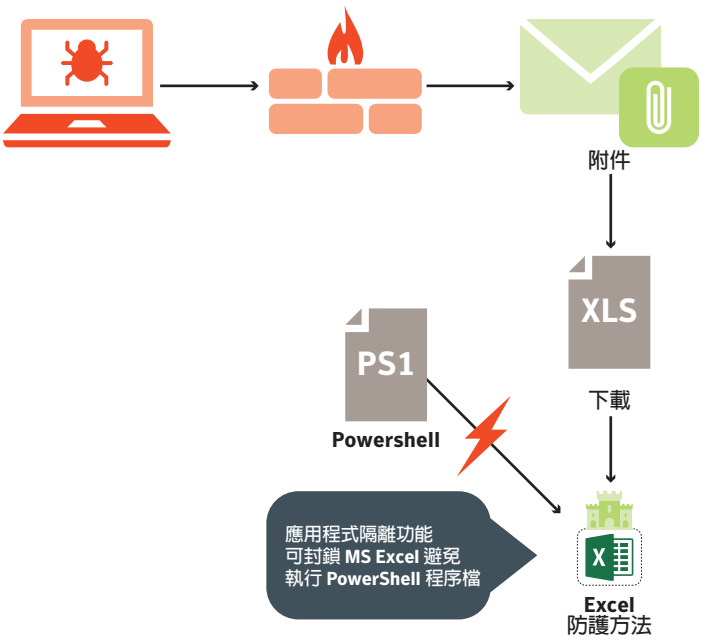
## 案例研討 2：透過應用程式隔離功能的「Castle」模式，預防以 MS Excel 發動的無檔案攻擊

**問題**：山姆收到「魚叉式網路釣魚」(spear phishing) 的電子郵件，由攻擊者假冒他定期往來的廠商提供專案報價。郵件另有名為「QuoteForReview.xlsx」的附件，為可發動攻擊的文件。若以 MS Excel 開啟此文件，工作表和他常見的報價單並無不同。山姆上當之後，停用了 MS Excel 本身的「受保護的檢視」模式，並根據說明啟用了檔案巨集以顯示報價。複雜的巨集接著會執行 Visual Basic 指令碼，透過 XLS 檔案的程式碼片段建構 PowerShell 指令碼，再以 Windows PowerShell (為 Windows 上常用的系統工具) 執行指令碼。這個過程將啟動攻擊程序：PowerShell 指令碼溝通攻擊者架設的 Command & Control (C2) 伺服器，下載附加工具以入侵憑證、進行網路偵查，再搬移到其他端點。

**解決方案**：SEP Hardening 可避免「已知善意」應用程式對環境產生威脅。

**運作方式**：SEP Hardening 能以「入堡觀察」(Castle) 模式執行 Microsoft Excel，限制其行為並避免竄改。當山姆開啟了攻擊用 XLS 文件，Excel 就會執行該文件的內容。但只要 XLS 檔案企圖建構 PowerShell 指令碼檔案，或透過 PowerShell 公用程式執行指令碼時，「Castle」模式隨即封鎖整個作業；因為 MS Excel 不會允許建立特定類型的檔案，亦不會啟動任何可執行檔，特別是如 PowerShell 的指令碼工具更不可能。

**優點**：應用程式隔離功能可讓「無檔案」攻擊毫無用武之地，保護山姆的裝置並阻絕攻擊程序。



# 總結

現今的進階攻擊重點，已經逐漸將攻擊重心放在端點上既有的應用程式與工具。有效的端點安全策略，往往必須對完整的威脅程度圖譜提供防護。在整合了列入黑名單、列入白名單、應用程式隔離等功能之後，賽門鐵克現在提供多樣可見的控制功能，只為能跨整個威脅連續性提供不間斷的保護。

有了賽門鐵克，在威脅找到立足點並產生傷害之前，就已經先行找出威脅並阻止。可疑的應用程式往往是透過一般使用者、瀏覽器、電子郵件，或其他協作工具帶入作業環境，且會自動「入監隔離」而不致對端點造成傷害。若可入侵的應用程式正好又是一般使用者產能的核心，現在更能以「入堡觀察」模式執行之，即不需擔憂其入侵行為或無檔案攻擊。真正的端點零時差防禦，能讓您放心執行任何所需的應用程式，順利進行自己工作。

## 關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 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策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。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 www.symantec.com.tw。

**台灣賽門鐵克股份有限公司** | 地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室 |
電話：(02) 8726-2000 | 傳真：(02) 8726-2199 | www.symantec.com.tw



symc_wp_SEP_hardening_TW_v1e