白皮書

STAR 惡意程式防護技術

目錄

概述

安全技術與應變中心 (STAR：Security Technology and Response) 是賽門鐵克負責安全技術創新和開發的部門，主要解決五個領域的防護問題：檔案、網路、行為、信譽及矯正。

在賽門鐵克內部，安全技術與應變中心 (STAR) 監督針對所有惡意程式安全技術所付出的研究和開發心力。這些要素構成了賽門鐵克企業和消費性安全產品的核心防護能力。

包含安全應變在內的安全技術與應變中心 (STAR) 是由安全工程師、威脅分析師及研究人員所組成的全球團隊，負責為所有賽門鐵克企業與消費性安全產品提供基礎功能內容和支援。STAR 擁有遍佈全球的「應變中心」，可監控網路上超過 1.3 億部系統的惡意程式碼報告、接收 200 多個國家／地區共 24 萬部網路偵測器的資料，以及追蹤影響 8000 多家廠商超過 5,5000 項技術的 2,5000 多個漏洞。此團隊運用龐大情報開發並提供世界一流的安全防護。STAR 約有 550 名員工。

多年前，傳統防毒技術是為了保護端點免受攻擊而存在。但是近幾年威脅態勢大幅轉變，不再認為單靠以防毒為主的技術就足夠了。為了因應這種情況，STAR 開發出安全技術協同合作生態系統，可保護賽門鐵克的使用者免於惡意攻擊。

這些技術要防範的主要威脅媒介：

- 偷渡式下載和網路攻擊
- 社交工程攻擊--假冒的防毒／安全軟體和偽造轉碼器

- 傀儡程式和傀儡網路
- 非程序和植入式威脅 (NPT)
- 目標式攻擊，包括進階持續性威脅 (APT)、木馬程式以及一般惡意程式零時差威脅
- 採用偷渡式下載避開其他防護層的惡意程式
- 使用 Rootkit 技術隱藏的惡意程式

本生態系統是由下列五個協同合作的領域所組成：

- 檔案式防護因靜態檔案啟發式技術有了全新創新，因而持續扮演主要的防護角色。
- 網路式防護可偵測使用已知及未知漏洞進入使用者系統的時間。
- 行為式防護會監控惡意活動的動態行為，而非靜態特性。
- 信譽式防護可檢視檔案的中繼資訊，包括檔案存在時間的長短、來源、傳遞方式、存放位置等。
- 矯正機制涵蓋多項技術，可協助清理受感染的系統。

透過協同合作，每項技術的運作都能更有效率及成效，能夠判斷指定的情況是否懷有惡意。當每項技術獲悉程序或檔案的不同屬性時，便會和其他技術分享所獲悉的內容。例如：網路式防護技術可追蹤網路下載的檔案來源，並和其他技術分享此資訊。

您可在下列標籤找到每項技術類型更多的詳細資料。

檔案式防護 (File-Based Protection)

關於防毒檔案掃描程式的常見誤解是，為了判斷檔案為善意或惡意，掃描程式只會在檔案中尋找已知的特徵。實際上，新型防毒解決方案在尋找威脅時已經超越簡單的特徵比對，並採用一般和啟發式技術。事實上，最佳防毒引擎可提供多種方式來辨識已知和未知威脅。賽門鐵克的檔案式防護便是這類技術之一。

檔案式安全歷史悠久，是防護技術的其中一項基礎。STAR 持續投入和推動檔案式安全的創新，以便針對威脅態勢保持最新發展。將受感染的檔案置於目標電腦中，是威脅在首次攻擊後持續存在於電腦上的主要方式之一。正因如此，檔案式防護對於偵測、抵禦及移除客戶電腦上的威脅而言始終成效卓著。檔案式技術要防範的一般威脅媒介包括：

- 惡意程式和病毒
- 目標式攻擊，包括進階持續性威脅 (APT)、木馬程式以及一般惡意程式
- 社交工程攻擊--假冒的防毒／安全軟體和偽造轉碼器
- 傀儡程式和傀儡網路
- Rootkit
- 惡意 PDF 和 Microsoft Office 文件 (PowerPoint、Excel 及 Word)
- 惡意壓縮檔案
- 間諜程式與廣告軟體
- 鍵盤側錄程式

為了解決這些威脅，我們以四個元件構成檔案式防護技術的核心：防毒引擎、自動防護、「清除大師」(ERASER) 引擎以及啟發式技術 Malheur 和 Bloodhound。

一、防毒引擎

賽門鐵克獨特的掃描引擎廣泛部署在 3.5 億台以上的電腦中。這項穩定的高效能安全性技術可進階偵測最新威脅。此引擎可經常在現場透過 LiveUpdate 更新，以便密集回應全新威脅。如此可讓我們更新產品的偵測能力，無須更新整個產品。

二、自動防護

賽門鐵克的即時檔案掃描程式可偵測遭寫入或來自檔案系統的威脅。以核心層級編寫的「自動防護」是一項資源佔用率低的高效能掃描引擎，可在不影響使用者的情況下抵禦最新威脅。當檔案寫入機器磁碟時，會啟動「自動防護」，並使用防毒、

Malheur 及 Bloodhound 引擎掃描檔案。「自動防護」以低階方式執行時可攔截受感染的檔案，避免檔案執行並感染系統。除了檔案防護之外，「自動防護」還為進階分析信譽技術中的「下載鑑識」提供關鍵功能。

三、「清除大師：ERASER」引擎

賽門鐵克的「清除大師」引擎可藉由各種偵測技術針對在客戶系統中找到的威脅，提供修復和移除功能。「清除大師」也會負責檢查啟動時執行的驅動程式和應用程式是否懷有惡意。為了確保產品不會遭到 Rootkit 或其他惡意程式欺瞞，「清除大師」使用各種能夠迴避一般系統登錄和磁碟查詢的技術。這些技術都可讓「清除大師」直接登錄以及直接存取磁碟。

四、啟發式技術 Malheur 與 Bloodhound

除了特徵式偵測，我們還提供相關技術，可判定前所未見但具備惡意檔案常見特性的檔案。Malheur 和 Bloodhound 技術便具備這項啟發式的防護能力。啟發式特徵可根據檔案屬性、利用漏洞的嘗試次數，以及在已知惡意程式發現的其他常見動作，藉此偵測未知的惡意程式。

深入探討各項功能

下列各節說明上述核心元件固有的檔案式技術特色。

■ 廣泛支援各種檔案

壓縮檔案和其他檔案內嵌的檔案都是用來檢驗是否隱藏惡意程式最常見的檔案類型。分析檔案類型的部分清單包括：

DOC、.DOT、.PPT、.PPS、.XLA、.XLS、.XLT、.WIZ、.SDW、.VOR、.VSS、.VST、.AC_、.ADP、.APR、.DB、.MSC、.MSI、.MTW、.OPT、.PUB、.SOU、.SPO、.VSD、.WPS、.MSG ZIP、.DOCX、.DOCM、.DOTX、.DOTM、.PPTX、.PPTM、.PPSX、. PPSM、.XLSX、.XLSB、.XLSM、.XLTX、.XLTM、.XLAM、.XPS、.POTX、.POTM、.ODT、.OTT、.STW、.SXW、.eml、.MME、.B64、 .MPA、.AMG、.ARJ、.CAB、.XSN、.GZ、.LHA、.SHS、.RAR、.RFT、.TAR、.DAT、.ACE、.PDF、.TXT、.HQX。.MBOZ、.UUE、.MB3、.AS、.BZ2、.ZIP、.ZIPX

■ Unpacker 引擎

在某些情況下，惡意程式會使用「Packer」技術模糊自身檔案，企圖規避採用簡單的模式比對演算法進行的偵測。我們的 Unpacker 引擎可以：

- 解壓縮受影響的可執行檔。
- 識別數百種不同的 Packer 系列。
- 採遞迴方式解除封裝進行多重封裝的檔案，直到找到核心惡意程式。

■ 一般虛擬電腦 (Generic Virtual Machine)

GVM 可讓程式碼在使用沙箱的安全環境下執行。

- Java 或 C# 等位元組程式碼式系統，可以在不會造成系統當機或停止回應的情況下，以極為安全的方式，快速生產全新防護技術。
- 針對 Trojan.Vundo 等威脅運用相當複雜的啟發式技術。
- 全面掃描非傳統的檔案格式，例如：PDF、DOC、XLS、WMA、JPG 等。

■ 防變種病毒引擎 (Anti-Polymorphic Engine)

包括進階的 CPU 模擬技術，以誘騙變種病毒惡意程式現出蹤跡。

■ 防 Rootkit 技術 (Anti-Rootkit Technology)

賽門鐵克擁有 3 項不同的防 Rootkit 技術，專門尋找和移除 Tidserv 和 ZeroAccess 等最頑固的 Rootkit，應付 Rootkit 最常用的隱匿技術。這些技術包括：

- 直接存取硬碟磁碟區。
- 直接掃描登錄區。
- 掃描核心記憶體。

■ 防木馬程式引擎 (Anti-Trojan Engine)

包括進階的雜湊技術，只需數毫秒的時間便可同時掃描數百萬個木馬程式和間諜程式威脅。

- 找出和擷取已知包含惡意邏輯的主要檔案區域。
- 取得每個區段的加密雜湊，並在指紋資料庫內搜尋。
- 有了進階演算法，「防木馬程式引擎」只需數毫秒的時間，便可同步掃描數千萬個惡意程式品種。

■ 「光子」(Photon) 引擎

使用「模糊：fuzzy」特徵找出已知和全新未知惡意程式變種。

- 使用數十萬個模糊特徵同步掃描檔案，大幅提升掃描效能。
- 模糊特徵在全新惡意程式品種釋出時即可加以偵測。

■ 進階啟發式引擎 (Advanced Heuristic Engines)

集中偵測伺服器端的變異品種。

- 採用超過十餘種 (仍持續成長) 不同的啟發式技術，來搜尋不同可疑檔案特性。
- 所有可疑檔案都會根據賽門鐵克的信譽雲端及數位特徵信任清單進行交叉比對。
- 引擎使用內容調整啟發式技術的靈敏度，例如：相較於安裝的應用程式，啟發式技術更容易針對新下載的檔案產生懷疑。

網　路

網路式防護涵蓋多項技術，可在惡意攻擊將惡意程式導入系統之前先行攔截。網路式防護不像檔案式防護，必須等到在使用者電腦中實際建立檔案後才能採取行動，而是可以開始分析透過網路連線到達使用者電腦的內送資料流，並在威脅襲擊系統前先行攔截。

賽門鐵克網路式技術要防範的主要威脅媒介：

- 偷渡式下載與網路攻擊工具組
- 社交工程攻擊--假冒的防毒／安全軟體和偽造轉碼器
- 透過 Facebook 等社交媒體發動的攻擊
- 偵測惡意程式、Rootkit 及受到 Bot 傀儡程式感染的系統
- 模糊威脅防護
- 零時差威脅
- 未修補軟體漏洞防護
- 惡意網域和 IP 位址防護

本類別包含三個不同的防護技術：

一、網路入侵防範解決方案 (網路 IPS)

具有通訊協定感知能力的 IPS 可理解並掃描 200 多個不同的通訊協定。此 IPS 可聰明並精確地分割二進位和網路通訊協定，尋找惡意流量的跡象。這項情報可讓網路掃描更加精確，同時提供健全的防護。它的核心是一般攻擊攔截引擎，可針對漏洞提供防規避攻擊攔截功能。Symantec IPS 的一項獨特功能是，無須設定就能啟用立即可用的網路 IPS 防護功能。在預設情況下，每個 Symantec Endpoint Protection 12.1 及更新的版本都會啟用這項關鍵技術。

二、瀏覽器防護

此防護引擎位於瀏覽器內，可偵測出傳統防毒軟體和網路 IPS 方法偵測不到的最複雜威脅。現今許多網路式攻擊都使用模糊手法規避偵測。由於瀏覽器防護能夠在瀏覽器內運作，因此執行時可以查看去模糊化的程式碼，如此一來就能偵測並攔截防護架構中進行低層級檢查時遺漏的攻擊。

三、未經授權下載防護 (UXP)

在網路式防護層中，這最後一道防線可以在不必使用特徵碼的情況下，協助減少未知及未修補的漏洞，並針對抗零時差攻擊提供進一步的保障。

鎖定問題

這些網路式防護技術能夠共同解決下列問題。

■ 偷渡式下載和網路攻擊工具組

賽門鐵克的網路威脅防護技術運用網路 IPS、瀏覽器防護及 UXP 技術，攔截偷渡式下載並避免惡意程式進入終端系統。我們使用各種預防方式以及這些技術，包括一般攻擊程式攔截技術 (後續會說明) 和一般網路攻擊工具組偵測。無論受到攻擊的漏洞為何，一般網路攻擊工具組偵測會分析常見網路攻擊工具組的網路特性，並針對全新漏洞提供額外的零時差防護，以及網路攻擊工具組防護。網路攻擊工具組和偷渡式下載防護最棒的部分在於，會主動阻止默默感染使用者系統的惡意程式並且系統隔離；傳統的偵測技術通常會遺漏這類惡意程式。賽門鐵克會持續攔截通常任何其他方式偵測不到的數千萬個惡意程式變種。

■ 社交工程攻擊

由於我們的防護技術會監控呈現的網路和瀏覽器流量，因此能夠使用這項端點情報判斷是否出現假冒的防毒解決方案，或偽造轉碼器等社交工程攻擊。我們的技術能夠在社交工程攻擊出現之前先行攔截，阻撓他們試圖誘騙一般使用者的伎倆。大部分其他具競爭力的解決方案都沒有這項強大功能。我們的解決方案可阻止數百萬個攻擊；而如果放任這類攻擊執行，則其他傳統的特徵式技術通常也偵測不到。

賽門鐵克可運用網路威脅防護技術，攔截數億個社交工程攻擊。

■ 鎖定社交媒體應用程式的攻擊

社交媒體應用程式已成為和成千上萬好友即時分享私人生活與工作更新內容、有趣影片及資訊的管道。這種追求即時更新的態度和網路廣度，也意謂著會成為駭客的主要目標，並運用此管道進行感染。部分常見的駭客技術包括入侵帳戶並傳送垃圾郵件或惡意連結、誘騙使用者參加假冒的問卷調查，或是 Facebook「按讚綁架」(Likejacking) 攻擊 (引誘使用者按下隱藏在滑鼠游標附近的「按讚」按鈕所提供的連結以觀看影片)。無論您是否出於自願，都會即時對更新內容按讚。

賽門鐵克的 IPS 技術可以抵禦這類攻擊，通常會在使用者受到誘騙按下某內容之前先行阻撓。賽門鐵克使用網路式防護技術阻止流氓和惡意 URL、應用程式及詐騙。

■ 偵測惡意程式、Rootkit 及受到 Bot 傀儡程式感染的系統

瞭解網路中受感染電腦的所在位置不是很好嗎？我們的網路 IPS 解決方案具備這項功能，而且包含偵測和矯正可能已經略過其他防護層級的威脅。我們會偵測試圖「在背景連線中進行通訊」(phone-home) 或透過更新散播更多惡意活動的惡意程式和 Bot 傀儡程式。如此可向 IT 管理員保證企業安全無虞，提供他們清楚的受感染系統問題清單以進行調查。使用 Rootkit 方式隱藏 Tidserv、ZeroAccess、Koobface 及 Zbot 等病毒變種和頑固威脅，可以使用此方法偵測及阻止。

■ 模糊威脅防護

現今的網路式攻擊使用各種複雜手法，以隱藏或模糊攻擊行動。賽門鐵克的瀏覽器防護內建於瀏覽器中，可偵測出傳統方式通常偵測不到的高度複雜威脅。

■ 零時差和未修補漏洞

最新一項防護功能就是針對零時差和未修補漏洞提供多一層防護。我們使用無特徵碼的防護方式攔截系統 API 呼叫，並避免下載惡意程式，我們將此稱之為「未經授權下載防護 (UXP)」。這是「網路威脅防護」技術中的最後一道防線，可以在不必使用特徵碼的情況下，協助減少未知及未修補的漏洞。自 2010 後，此技術即隨附於產品並且會自動啟用。

■ 未修補軟體漏洞防護

惡意程式通常會透過入侵軟體漏洞的方式默默地安裝在系統上。賽門鐵克的網路防護解決方案提供多一層的防護，稱之為「一般攻擊程式攔截」(GEB) 技術。無論系統是否完成修補，GEB 會「普遍」提供基礎漏洞攻擊防護。Oracle Sun Java、Adobe

Acrobat Reader、Adobe Flash、Internet Explorer、ActiveX 控制項或 QuickTime 中的漏洞，在現今的威脅態勢中十分常見。我們透過逆向工程瞭解入侵漏洞的方式，並且在網路上尋找入侵特徵，藉此打造「一般攻擊程式攔截」防護，實際提供網路層級的修補程式。一項單一的 GEB 或漏洞特徵，就可防範賽門鐵克或其他安全廠商前所未見的數千個惡意程式變種。

■ 惡意 IP 和網域攔截

賽門鐵克的網路式防護也包含惡意 IP 和網域攔截功能，可杜絕來自已知惡意網站的惡意程式與惡意流量。賽門鐵克運用安全技術與應變中心團隊的分析來尋找惡意網站，並透過 LiveUpdate 進行更新，以針對不斷變化的威脅提供即時防護。

■ 已改善的防規避能力

已新增額外的編碼支援以改善偵測成效，並且在使用 base64 和 gzip 等一般技術進行編碼時也能改善防攻擊規避的能力。

■ 針對政策運用強制執行和資料外洩辨識進行的網路稽核偵測

網路 IPS 可用以辨識可能違反企業使用政策，或是透過網路用來阻止資料外洩防護的應用程式和工具。也能偵測、警示或預防即時通訊、點對點、登入以開啟分享、社交媒體等流量以及其他「有意思的」流量。

■ STAR 情報通訊匯流排 (Intelligence Communication Bus)

網路防護技術無法自行運作。此引擎運用 STAR 情報通訊協定 (STAR ICB) 和其他防護技術共用情報。網路 IPS 引擎能與賽門鐵克 SONAR 引擎和 Insight 信譽引擎通訊，提供其他安全公司無法提供的知情與準確防護。

行為型防護

現今有數百萬名使用者受到誘騙按下偽裝成影片播放程式的惡意程式，或是只會感染使用者以及藉由社交工程方式誘騙使用者支付費用購買毫無用處的軟體之流氓防毒應用程式。偷渡式下載和網路攻擊工具組會默默地感染造訪主流網站數以億計的使用者。有些惡意程式會在執行的程式和系統程序中安裝 Rootkit 或植入惡意程式碼。現今的惡意程式可採取動態方式產生，使用檔案式偵測保護一般使用者系統已然不足。

為何需要行為式安全？

在 2010 年，賽門鐵克觀察到超過 2.86 億個惡意程式變種，並攔截超過 30 億次攻擊。隨著惡意程式威脅和變種持續成長，賽門鐵克瞭解到無論一般使用者執行哪些行為或是惡意程式如何進入一般使用者的系統，都需要建立領先業界的創新方法來避免惡意程式感染，並在背景中自動保護使用者。賽門鐵克的 Insight 信譽技術和我們的 Symantec Online Network for Advanced Response (SONAR) 行為式安全，便是這一類的兩項創新方式。

由於行為可以推廣各種惡意檔案和非惡意檔案，成效比檔案式啟發式技術還要好，因此行為式安全技術最適合因應這種快速成長的速度。若要改變行為勢必大費周章，否則難以改變或者無法輕易改變，而行為改變則不利於惡意程式的散佈和建立策略。

行為式防護技術可提供有效且非侵入式的防護，防範之前未發現的零時差電腦威脅。SONAR 解決方案可根據應用程式的行為 (而非應用程式的外觀) 提供威脅防護。SONAR 是行為式技術和功能的主要引擎：此分類引擎是以人工智慧、人工編寫的行為特徵以及行為政策鎖定引擎為基礎。結合這些元件後可提供領先業界的安全防護，防範最常見的社交工程和目標式攻擊等威脅。

賽門鐵克行為式技術要防範的主要威脅媒介：

- 目標式攻擊，包括進階持續性威脅 (APT)、木馬程式、間諜程式、鍵盤側錄程式以及一般惡意程式
- 社交工程攻擊--假冒的防毒／安全軟體、流氓金鑰產生器和偽造轉碼器
- Bot 傀儡程式和傀儡網路
- 非程序和植入式威脅 (NPT)
- 零時差威脅
- 採用偷渡式下載避開其他防護層的惡意程式
- 使用 Rootkit 技術隱藏的惡意程式

賽門鐵克行為式技術層何時會提供防護？

無論使用者是否有意 (受到社交工程誘使) 執行惡意應用程式，或惡意程式透過偷渡式下載等網路式攻擊企圖悄悄地自動安裝，只要惡意程式執行或是開始或嘗試將自己植入執行的程序時，SONAR 都會即時阻止惡意程式感染系統 (NPT)。SONAR 能夠針對 Hydraq ／ Aurora、Stuxnet 以及 Tidserv 與 ZeroAccess 之類的惡意程式嵌入式 Rootkit 提供零時差防護，在在顯示 SONAR 是端點防護不可或缺的技術。

如何運作？以人工智慧為基礎的分類引擎

賽門鐵克已建立世界級的大規模行為設定檔資料庫之一，其內容涵蓋將近有 12 億個應用程式執行個體。賽門鐵克藉由使用電腦學習分析方式分析善意和惡意應用程式行為的屬性，因此得以針對尚未建立的應用程式行為建立設定檔！ SONAR 分類引擎仰賴將近 1,400 個不同的行為屬性，以及收集自 Insight、IPS 及 AV 引擎等其他端點安全元件的豐富內容，因此能夠迅速找出惡意行為並採取行動移除惡意應用程式，以免造成危害。在 2011 年，SONAR 為賽門鐵克客戶分析超過 5.86 億個可執行檔、DLL 及應用程式。

非程序式威脅防護

現今的威脅不單只是獨立的惡意程式可執行檔而已。這些威脅會盡早在植入常見執行程序、應用程式，或是將元件登錄到可擴充應用程式時隱藏，並代表受信任的作業系統程序或應用程式掩蓋其惡意行動。舉例來說，惡意程式執行時可以將惡意程式碼植入 explorer.exe (桌面 Shell 程序) 或 IExplorer.exe (Internet Explorer 瀏覽器) 等執行中的程序，或是以這類應用程式的附檔名登錄惡意元件。此後惡意活動會以知名的受信任作業系統元件的面貌出現。SONAR 會藉由為嘗試植入的來源程序進行分類，防止程式碼植入目標程序。除了分類，必要時也會防範惡意程式碼在目標／受信任的程序中載入或執行。

行為政策鎖定

偷渡式下載會透過攻擊瀏覽器外掛程式漏洞的方式進行，例如：Adobe Reader、Oracle Sun Java 及 Adobe Flash。漏洞遭到攻擊後，偷渡式下載便可取得容易遭到攻擊的應用程式，並悄悄地啟動任何想啟動的應用程式。我們透過建立行為政策鎖定定義的方式，攔截各種惡意行為，例如：「Adobe Acrobat 不應建立其他可執行檔」或「不允許在 explorer.exe 程序中植入 DLL」，藉此保護系統。這可描述為根據政策或規則鎖定行為。這些 SONAR 定義／政策是由賽門鐵克 STAR 團隊所建立，並以攔截模式自動部署，無須由客戶管理。如此一來可避免善意應用程式的可疑行為，自動為使用者提供防護。

強制執行行為政策 (BPE) 特徵

隨著不斷變更的威脅態勢進化是 SONAR 技術不可或缺的一環，我們也因而得以鎖定日後的各種威脅，藉此擴大防護能力。當我們觀察到全新 Rootkit、Trojan、假冒的防毒／安全軟體或其他類型的惡意程式等全新系列威脅時，當下便可建立新的行為特徵，無須更新產品程式碼就可偵測全新系列威脅並加以發佈。這是所謂的「SONAR 強制執行行為政策特徵」。這些特徵可快速撰寫、測試及部署，並賦予 SONAR 彈性和適應力，以及極低的誤報率因應某些類別的新興威脅。我們擁有許多 SONAR BPE 特徵，能夠針對 Graybird、Tidserv、ZeroAccess 及 Gammima 等特定惡意程式威脅和 Rookit、鎖定假冒的防毒／安全軟等誤導型應用程式。

那麼 BPE 特徵如何運作？

讓我們來檢視一下執行的應用程式。

- 在 Windows 暫存目錄放入某些元件
- 新增各種登錄項目
- 變更主機檔案
- 沒有使用者介面
- 開啟高連接埠的通訊

以上任何一項行為單獨來看都不算「惡意」行為，但整體而言這樣的行為概況便屬於「惡意」。我們的 STAR 分析師會建立這樣的規則：如果看到這些行為以及具備某些 Insight 信譽特性的可執行檔，就應阻止該程序執行並回復變更--SONAR 能夠在受感染但合法的應用程式周圍執行虛擬沙箱，如此一來可避免受感染的應用程式採取任何可能危害使用者電腦的惡意動作。這種運用應用程式行為以及行為方式，而非外觀的手法，是端點安全防護中相當新穎的典範。

運用沙箱自動矯正惡意檔案

當應用程式、程序及活動活絡時 (而非靜態)，即時行為防護引擎可加以監控並以沙箱執行。可以執行系統變更回復作業，避免惡意活動影響系統。

即時監控應用程式和程序

SONAR 可監控和保護 1,400 多種各項執行中的應用程式、DLL 及程序，並在執行時提供即時威脅防護。

STAR 情報通訊匯流排

SONAR 技術無法自行運作。此引擎運用 STAR 情報通訊協定 (STAR ICB) 和其他防護技術共用情報。SONAR 引擎能與網路 IPS、AV 及 Insight 信譽引擎通訊，提供其他安全公司無法提供的知情與準確防護。

信譽型防護

信譽式安全是 STAR 開發的防護技術套件最新附加功能，能夠因應威脅態勢的最新發展 (微分佈惡意程式)。我們的信譽系統結合超過 1.3 億名貢獻使用者的智慧，根據使用者的匿名採用模式學習分辨善意和惡意應用程式。然後使用這項情報自動針對全世界幾乎所有的軟體檔案進行分類。所有賽門鐵克產品都會運用這項信譽資料自動攔截全新惡意程式，並反過來辨識和允許全新的合法應用程式執行。

問題：不斷變更的威脅態勢

幾年前散佈到數百萬台電腦的威脅數量相對較小。透過部署至各受防護的系統之單一防毒特徵便可輕鬆阻擋每項威脅。惡意程式作者因瞭解到這一點而轉換技術，如今使用各式各樣的模糊技術快速改變他們生產的威脅外觀。攻擊者針對個別受害者或少數受害者即時建立全新威脅變種已是常態，因此每年都有數億種不同的全新變種產生。

這些威脅會透過網路式或社交工程攻擊散佈到目標電腦。我們的資料顯示，現今大多數的威脅在全球破獲的電腦不到 20 台，讓安全性公司幾乎無法瞭解大部分的威脅、取得樣本、進行分析以及編寫傳統的反應特徵碼。每天建立的全新變種超過 60 萬個 (去年賽門鐵克從保護的客戶電腦中收到 2.4 億個唯一威脅雜湊)，根本無法建立、測試及發佈解決問題所需、如此大量的傳統特徵碼。

解決方案：信譽式防護

傳統的病毒特徵比對需要安全廠商取得每個威脅樣本才能提供防護。賽門鐵克的信譽式安全則採取截然不同的方法。我們不著眼於惡意檔案，而是嘗試精確分類所有善意和惡意的軟體檔案，分類依據則是全球各地每天時時刻刻傳給賽門鐵克、無以計數的匿名遙測「Ping」。這些幾乎即時的 Ping 能讓賽門鐵克瞭解：

- 客戶電腦上部署的應用程式 (每個應用程式都會依其 SHA2 雜湊進行唯一識別)。
- 網路上的應用程式來源。
- 應用程式是否採用數位簽章。
- 應用程式存在時間的長短。
- 各種其他屬性。

我們會透過全球智慧型網路、安全機制應變中心，以及提供應用程式執行個體給賽門鐵克的合法軟體廠商新增這項資料。

和 Facebook 社交網路不同的是，這項資料會併入大規模模型當中，並由應用程式和匿名使用者之間的連結所組成，不單只是使用者之間的連線而已。此方式可將所有檔案和數百萬名匿名使用者之間的關係進行編碼。接著我們會分析此一由應用程式與使用者構成的網路，以推演出每個單一應用程式的安全等級，藉此辨識每個應用程式為善意、惡意或介於兩者之間。目前本系統追蹤超過 25 億個善意和惡意檔案，每週發現的全新檔案超過 2200 萬個。

特色

賽門鐵克用戶端、伺服器及閘道產品使用「信譽」資料協助改善防護其能力，採用的方式有以下四種：

■ 卓越的防護能力

信譽系統可針對每個單一的善意或惡意檔案，運算出高度準確的信譽等級。這不僅對於對抗流行的惡意程式相當有效，也可辨識最隱晦的威脅，即使這些受影響的使用者只是整個網際網路中的少數人。此方式可提升所有惡意程式類別的偵測率。

由信譽提供的防護能力最明顯的提升層面在於相關產品的「下載鑑識」(DI) 功能，以及 Symantec Endpoint Protection 產品的「下載顧問」(DA) 功能。DI/DA 可在每個全新可執行檔從網際網路下載時予以攔截。接著會查詢賽門鐵克信譽雲端取得評等。DI/DA 會根據從雲端獲得的評等，採取下列三種動作的其中之一：

- 如果確認檔案的信譽不良，會直接攔截。
- 如果確認檔案的信譽良好，就會允許執行。
- 如果仍在確認檔案信譽，而且無法得知是否安全，會警告使用者該檔案尚未獲得證實。使用者可根據個人對風險的容忍度，決定是否要使用該檔案。在企業部署情況下，管理員也可依據每個部門的獨特風險容忍度，針對不同部門指定不同的攔截／允許門檻。

■ 防止誤報

這項技術的兩個獨立層面均可進一步降低賽門鐵克對於合法軟體已大幅降低的誤報率：

首先，由於信譽式技術會根據社交採用圖 (而非每個檔案的內容) 衍生出檔案評等 (例如：傳統的防毒掃描技術)，因此可做為是否擴增防毒啟發式技術或行為攔截等傳統偵測技術的第二參考意見。如果這兩種方式均顯示該檔案為「惡意」檔案，則誤報的可能性便會非常低。

再者，由於系統會保留所有可執行檔內容的普及率資訊，這項資訊也可作為判別是否具有惡意之決策的依據。舉例來說，相較於存在於數百萬台電腦的檔案，只存在於全球兩個系統的檔案，其破壞力在判定上會遠不及前者。將此資訊納入每個決策，可做出更能保護使用者的明智決定。

■ 強化的效能

一般使用者的電腦都有數千個檔案從未變更過 (也有少數例外狀況)，而這些檔案都是善意檔案。但是由於傳統防毒技術會根據已知的惡意威脅清單專注尋找惡意檔案，所以必須掃描使用者系統內的每個檔案，逐一比對已知威脅清單的內容。發現新威脅時，必須以全新特徵碼重新掃描使用者系統中的每個檔案，查看該檔案是否符合任一新發現的威脅。

當您想到安全性廠商每天會發佈數千個全新病毒特徵碼時，這樣的程序毫無效率可言。然而，信譽式安全在設計階段便針對所有善意和惡意檔案設定精確的安全評等。此舉可讓擁有信譽技術的產品掃描使用者系統時，明確將已知的善意檔案標示為善意後便不再理會；除非檔案內容變更，否則不會重新掃描。此舉可大幅提升效能、減少傳統掃描所需的資源，並提供高達 90% 的即時防護能力，有效改善使用者體驗。

■ 政策式鎖定

傳統的安全解決方案著重在以二進位方式攔截已知的惡意程式--明確辨識為惡意的任何檔案都會從使用者電腦中移除，其他則獨立保留 (無論是否確實為惡意)。事實上，常見的情況是惡意程式在使用者系統裡仍有其立足點，這些狀況仍尚待解決。想像網路罪犯剛建立一個全新惡意程式，而廠商還未有機會能先行分析這樣的威脅，因此現有的防毒特徵碼極可能無法偵測到這類威脅。除非這項全新威脅入侵已知漏洞或表現出預定的可疑行為模式，否則現有的安全技術可能無法偵測到。信譽式安全可協助使用者與 IT 管理員因應這種情況，方法是讓他們針對能夠在其電腦上執行的內容做出更完善而且明智的決策。

除了管理檔案是否為善意或惡意的相關資訊外，賽門鐵克的信譽式系統也會保留其他屬性，例如：每個檔案的普遍性和存在時間。在即將推出的企業產品中可使用這些屬性執行政策，讓管理員掌握使用者系統可安裝的項目。例如：萬一遇到全新威脅，即便未標示為惡意，該威脅的存在時間也非常短，而使用者和 IT 管理員也可使用信譽資訊執行電腦上許可內容的相關政策。另一個例子是，IT 管理員可能限制財務部門的員工，可以下載的應用程式必須至少有 1000 名認證使用者、網際網路上供應的時間至少兩週；而 IT 服務台人員可以下載的檔案，則是至少有 100 名認證使用者、信譽評分中等且存在時間不限。這些政策都可讓管理員根據每個部門的獨特風險容忍度，量身打造防護能力。根據我們的研究顯示，這個方式可大幅降低企業內部暴露在全新惡意程式的風險。

矯　正

雖然我們的目標是避免威脅進入電腦中，但現實狀況是仍有使用者的系統受到感染。這類情況可能包括：

- 使用者原先未安裝安全性產品。
- 使用者的產品訂閱授權已過期。
- 使用者遭受全新零時差威脅的攻擊。

賽門鐵克的矯正技術可提供各種功能清理受感染的電腦，協助解決這些狀況。這套核心技術內建在我們所有的惡意程式安全產品之中。

最近我們推出一套獨立工具，可協助矯正更激進的感染。這些工具包括賽門鐵克強力清除器 (隨附在 Symantec Endpoint Protection 支援工具中)。矯正工具的特色包括：

■ 可輕鬆更新的靈活引擎

為了規避安全套件的偵測，威脅涉及的範圍不斷改變，這些工具可輕鬆更新，以便因應全新的零時差威脅。

■ 全力鎖定感染目標

從下載程式到酬載以及提供隱匿功能的 Rootkit，現今的感染狀況相當複雜，駭客會運用多項元件協調出有利可圖的結果。經過仔細調整的強力清除器引擎，除了可尋找威脅本身的行為模式外，還可找出起初將威脅導入系統的下載程式，藉此偵測和移除這些風險。

■ 積極主動的偵測技術

為了偵測各式各樣的威脅，強力清除器引擎運用多個全新啟發式引擎和資料分析點。這些包括 Packer 啟發式技術、載入點分析、Rootkit 啟發式技術、行為分析、散佈分析以及系統設定監視器。

防毒軟體的 5 大技術很重要，但不是資訊安全的全部

不管是電腦安全、網路安全亦或是資訊安全，在這些大家耳熟能詳卻未必了解透徹的範疇裡，防毒軟體總是扮演非常重要的角色。防毒軟體的定位就是假設有惡意程式已經正在攻擊或者是剛開始嘗試攻擊電腦，也就是正在攻擊中或是發動攻擊的初期階段，它能夠發揮作用，將惡意軟體攔截下來，以避免後續衍生的連環效應。本文分享的賽門鐵克安全技術與應變中心 (STAR) 所提供的大類技術是在這種情境裡面非常先進的防護技術，而且也會隨時更新並與時俱進。

隨著資安事件呈指數成長以及駭客技術的進化，防護機制與政策也必須與時俱進更要領先敵對的威脅者，現階段最完善的防護機制是拆解整個攻擊鏈，不管從美國國家標準技術研究所（NIST）所規範的五階段的框架，還是拆解洛克西德馬丁公司所註冊的網路攻擊鏈七步驟，在不同的階段都有應對的防禦機制，完善的安全防護機制應該在攻擊前、攻擊中、入侵中以及入侵後提供最佳的預防、保護、回應以及復原，以提升最完整的端點安全等級與範圍。

首先，在「攻擊前」如能降低攻擊面，也就是把威脅向量 (Threat Vector) 降低，所謂的威脅向量就是威脅可利用的路徑或方法。所以禁止或限縮已知風險的來源，例如：禁用隨身碟、禁用私人設備連入公司內網、強密碼、隨時更新修補、禁用公司設備透過實體或無線連入外網或非公司裝置、不在公司電腦開啟私人郵件或處理非公務的作業、不安裝來路不明的軟體、在郵件系統安裝過濾與防護機制、網頁安全過濾與分類、網路分割與職責分離…，這些都是預防的機制，科學數據顯示在預防階段的投資效益至少是善後處理成本的 10 倍以上， 還不包含商譽損失以及後續法規的罰則。在預防階段如果能從長計議，好好規劃與執行其實就是應驗事半功倍的最佳樣本。

其次，如果惡意程式已經正在發動攻擊或者是剛開始嘗試攻擊也稱為「攻擊階段」，這個階段就是防毒技術該發揮效應的時刻。也是這一篇文章裡面描述的基於檔案、網路、行為、信譽及矯正的防護技術所擅長的範疇。在「攻擊前」的預防階段，如能妥善規劃與執行，其實可大大降低這階段需要防毒技術需要處理的事件， 也能提高電腦的工作效能。

再來，萬一前兩個階段的預防以及防護機制都失效時，也就是已經被入侵但尚未釀成大禍時，也就是「入侵階段」有那些技術是可以在第一時間發現被入侵的徵兆。在這階段入侵者會很有計畫地長期蟄伏，並規避防護機制的偵測，或利用正常的檔案存取或網路連線來偷渡非法行為。這個階段基本上就是亡羊補牢階段，要把損失降到最低。

最後，這個階段稱為「入侵後階段」， 最糟糕的狀態就是企業內部的資料都被搬光了，或是所有的電腦都被加密了，還釐不清整個事件的來龍去脈、更找不出真正的兇手或是相同的災難一再發生。威脅者會將電腦的日誌清除，讓整起事件的調查鑑識無從下手。在這個階段基本上就是能保存完整詳盡地的入侵紀錄以重塑犯罪現場來加快事件分析以及快速恢復到原來可運行的狀態，並避免再次受到攻擊。

賽門鐵克端點安全，比你想像的更完整

完善的資安策略必須建基在穩固與平衡的基於安全管理、防護技術以及人員資安認知能力 (People、Process & Technology) 提升的全方位思維。特別是人員的資安認知能力以及警覺性更是重要。企業三令五申要求不要在公司內部收發私人信件、不要瀏覽與工作無關的網頁、不要開啟不明寄件者之的郵件，不要點擊來路不明的鏈結、不要開啟不是你所期待的附件、不要使用來路不明以及非法的軟體、不要將帳號／密碼提供給任何人使用、禁用隨身碟、只要覺得是可疑的惡意郵件或網路釣魚就要馬上回報…。但郵件的寄件者身分非常容易偽裝，非專業人士很難分辨真偽。經過精心設計的郵件的主旨及內容也非常容易誘惑或迫使受害者開啟惡意郵件。無論佈署多麼先進的防護技術來實作網路安全，利用人的純真的天性和對人性的信任去營造情境的社交工程攻擊，總能突破這些號稱銅牆鐵壁、固若金湯的防禦技術，而抵禦社交工程攻擊最好的防禦就是警覺心。

保安資訊團隊專注在資訊安全領域超過二十年，對於資訊基礎架構的理論基礎與運作原理有非常透徹的理解與分析能力，特別熟稔賽門鐵克資安解決方案的工作原理以及效益最大化。就整個攻擊鏈：「攻擊前」、「攻擊階段」、「入侵階段」、「入侵後階段」的四個不同階段，賽門鐵克都有非常完整的可應對防護技術與預防方案。在端點這個面向，即使是一直被稱為企業版的防毒軟體的標準端點安全軟體：SEP(賽門鐵克端點防護-- Symantec Endpoint Protection)，其實它的功能不只是防毒軟體，它有好幾項大大超越防毒軟體的功能包括：「應用程式控管」、「裝置控管」、「系統鎖定」以及「主機完整性檢查」。「應用程式控管」：限縮特定的應用程式才能安裝或執行，所以套用良好政策的情境，即便是已經被惡意程式入侵，也無法發作。裝置控管 : 能強制鎖定除鍵盤滑鼠外，完全不接受隨身碟等任何 USB 裝置，既能減少惡意程式感染也能避免資料透過隨身碟流出，孰悉此運作原理的技術顧問更能依情境微調或客製許多有助於管理或安全的實作政策。強大的「主機完整性檢查」，運作原理就是可依檢查系統的現有狀態與要求條件做比對，只要不符合要求條件的，就會採用相對應的風險隔離或降低動作，跟我們寫程式的 iF…Then…Else 的運作原理很相像。比方講，更新或修補沒上到特定的版次，就不能網路存取，即便存取內網也不行，甚至直接關機。或是病毒定義檔沒更新到最新的、或是沒有登入到 AD 的、或是還在使用微軟已經停止支援的作業系統…。

不在防毒軟體五大技術範疇的強大技術還包含：「主機型防火牆」具備網路層及應用層防禦及管理功能，防止任何未獲授權的使用者存取組織中連線到 Internet 的電腦網路、監控您的電腦與 Internet 上其他電腦之間的通訊、建立防護措施，允許或攔截他人企圖存取您電腦上的資訊、警告您來自其他電腦的連線嘗試警告您電腦上的應用程式嘗試連線到其他電腦。「入侵防護」支援已公開之漏洞型攻擊，類似行為之零時差攻擊亦能防護，並支援無檔案型態 (Fileless) 及記憶體攻擊。「竄改防護」防護軟體自身避免被停用的保護功能，常見的大規模入侵，第一個動作就是停用安全軟體 (防毒軟體)，就如同先把監視系統先破壞的強盜案一樣，SEP 的「竄改防護」可以第一時間發現 SEP 異常的停用，更可有效避免這種大規模被攻陷的風險。

這篇文章的重點僅針對賽門鐵克的防毒技術的五大範疇做說明，也稍微介紹大家一直稱呼的企業版的防毒軟體的標準端點安全軟體：SEP 的額外防護技術及預防機制。其實，賽門鐵克還有一個業界最完整的端點安全方案，稱為「端點安全完整版」-- 簡稱 SESC (Symantec Endpoint Security Complete)，它涵蓋整個攻擊鏈：「攻擊前」、「攻擊階段」、「入侵階段」、「入侵後階段」等四個不同階段所需的防護技術，是物超所值的端點安全完整組合。SESC 除具備 SEP 的所有功能外，還具有「EDR(端點偵測與回應)」的功能，EDR 的運作原理是透過系統及安全日誌的關聯分析與交叉比對，並且參照全球的威脅情資透過後端 AI 平台與專業威脅分析團隊工程師的協作，可以早期發現目標式攻擊以及網路駭客集團的攻擊並建議安全管理團隊採取合適的處理措施，大大降低回應資安事件束手無策以及想破頭的燒腦時間，特別是中小企業無法負擔足以應付處理資安事件分析的高階人力成本以及高階人力使用傳統工具的工作過度負擔的人員異動風險。除 EDR 外，SESC 還有基於端點的「AD 防護」功能，有別於傳統在 AD 主機築高牆的防護 AD 機制，Symantec Endpoint Threat Defense for Active Directory，比較像是零信任的端點防護 AD 機制，讓每個端點都成為保護 AD 的戰士。另一個重要且領先業界的「Adaptive (自適應) Protection：防護技術」，它能有效規範每個應用程式的行為，避免常用的管理工具成為駭客利用的凶器。…更多詳細的 SESC 說明可參考專屬網頁或型錄下載。

賽門鐵克郵件安全，業界最強大、功能最完整

在郵件安全方面，大家對賽門鐵克的印象可能還停留在 2015 年前，垃圾郵件氾濫的全盛時期的高攔截率 (99%) 以及低誤報率 (低於百萬分之 1) 的 Brightmail Anti-Spam 印象。Symantec 透過不斷併購新創公司與整合現有技術，我們現有的地端自建「郵件主機安全方案」：Mail Security for Microsoft Exchange 以及「郵件安全閘道」：SMG(Symantec Messaging Gateway) 兩者除承襲在過濾 Spam 的效率與有效性的 DNA 外，對於惡意郵件、目標式攻擊郵件、商務電子郵件詐騙 (BEC) 都有專家一致推崇的防禦能力。

另一項重量級的「郵件安全雲端服務」：Symantec Email Security.Cloud 除非有特殊考量或受限於罕見架構無法採用雲端服務，否則它就是最好的、最完整的郵件安全解方案。地端自建郵件安全方案所有的安全它都有，更受惠於雲端架構的「高運算能力」與「高擴充延展性」，它的即時反應時間比地端有明顯感受得到的效益。其他值得一提的功能包括：「即時鏈接檢查」、「威脅隔離」、「沙箱」、「郵件 ATP ／ ETDR」，連最需要但很難取得的資源：「人員的資安認知能力的提升」以及平常的演練測試的教育訓練機制，賽門鐵克的郵件安全雲端都包含。

資安事件超過一半都是透過電郵件來的，所以不要點擊惡意連結及開啟惡意附件最是重要也最容易出錯，透過社交工程的惡意電郵尤甚，透過偽裝發信者來濫用人性善良、緊急事件的壓力、權威信任…，讓點擊惡意連結及開啟惡意附件成為早晚一定會發生， 而不是會不會發生的問題，即便安全專家也是人，也一樣會中計，只是機率比較低。

「即時鏈接檢查」會去檢查每一封電郵內帶的網址 URL，並經過安全強化處理後讓每個鏈接轉向到 Symantec 的安全存儲空間，即便經過一段時間後，該 URL 的最終連結已經變更 N 次了，它還是每次都檢查，而且是檢查到最終的目的端。駭客現在會在初始的 URL 安分地不放置惡意連結以躲過安全檢查，但過一段時間後，就會透過鏈接的多次再轉向，最終轉到惡意的網址，一般的安全檢查只會在第一次收到郵件時做檢查，已經收進來的郵件的 URL 再一次點擊完全不會檢查。

而「沙箱」是用來檢查附件及鏈結的，作為防毒軟體的補強及惡意程式的預先觸發引爆機制，避免客製化的惡意程式先行驗證主流防毒軟體無法偵測到再釋出以提高成功率並避免打草驚蛇。「威脅隔離」的作用是：當有一封電郵，它看起來很重要，但我不知道它安不安全， 所以賽門鐵克就提供了一個稱為遠端瀏覽的防護技術，讓該電郵在賽門鐵克的一次性隔離空間上來執行，只把執行後的結果畫面傳送回來給使用者，對於需要填寫資料的互動式網頁，也可以設定為唯讀模式，不能填寫任何資訊。

「郵件 ATP ／ ETDR」：可以早期發現目標式攻擊，避免小問題演變成大災難，它可以協助安全管理人員，以減輕事件分析的負擔及加快處理時間。就如同在端點上的 EDR 運作原理一樣，這個領域的工作原理都是： 透過系統及安全日誌的關聯分析與交叉比對，並且參照全球的威脅情資透過後端 AI 平台與專業威脅分析團隊工程師的協作，可以早期發現目標式攻擊以及網路駭客集團的攻擊並建議安全管理團隊採取合適的處理措施，大大降低回應資安事件束手無策以及想破頭的燒腦時間，特別是中小企業無法負擔足以應付處理資安事件分析的高階人力成本以及高階人力使用傳統工具的工作過度負擔的人員異動風險。我們有內部實測的與友商比較的比較數據，您也可以下載型錄、簡報檔以及內部實測的比較數據說明。

> 賽門鐵克「網頁安全」，CP 值最高的八合一的套餐方案，讓企業無後顧之憂
> 詳細資訊請參考 型錄 或與 保安資訊 聯繫

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/enterprise-security/enterprise-security-solutions 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