保安資訊--今日最新(台灣時間2025/02/25)
賽門鐵克原廠防護公告重點說明

前言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告 (Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS)的好處 (以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 37 萬 6,800 台受保護端點上總共阻止了 4,730 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2025/02/24)**

- 在**7萬9,500**台端點上，阻止了**1,700**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬4,200**台端點上，阻止了**660**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,700**台**Windows**伺服主機上，阻止了**720**萬次攻擊。
- 在**4萬9,300**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,600**台端點上，阻止了**78萬8,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,800**台端點上，阻止了**270**萬次嘗試利用的應用程式漏洞。
- 在**10萬6,000**台端點上，阻止了**230**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,600**台端點上，阻止了**83萬9,900**次加密貨幣挖礦攻擊。
- 在**10萬5,200**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**502**台端點上，阻止了**7萬6,200**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 14 萬 8,400 個受保護端點上阻止了總計 770 萬次攻擊。**(2025/02/24)**

- 使用網頁信譽情資，在 **141.6K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **19K** 個端點上 **336K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **5.7K** 個端點上攔截 **123.2K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **182** 個端點上攔截 **5K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

點擊此處獲取--關於賽門鐵克原廠防護週報

2025/02/24

SectopRAT遠端存取木馬(RAT)，偽裝成Chrome瀏覽器的安裝程式來散播

SectopRAT 遠端存取木馬 (RAT)(也稱為 ArechClient2) 是一款基於 .NET 多功能惡意竊密程式，用來竊取受害者機器上的敏感資訊。在真實網路情境上已經觀察到散播此惡意軟體的新一波行動。攻擊者最近將其偽裝成 Google Chrome 瀏覽器安裝程式，透過濫用 Google Ads 平台散佈此多功能惡意竊密程式。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Ps-Msbuild!g1

基於行為偵測技術(SONAR)的防護：
- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g349
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：
- Downloader.Trojan
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：
- System Infected: Bad Reputation Application Connecting to Cloud Storage
- System Infected: Trojan.Backdoor Activity 812
- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/02/24

惡意捷徑檔. LNK被用作惡意行動的工具，鎖定教育機構的散播Lumma惡意竊密程式

據報導，有惡意軟體利用教育機構的基礎架構散佈 Lumma 惡意竊密程式。此攻擊始於偽裝成 PDF 文件的惡意捷徑檔. LNK，來引誘受害者。一旦執行，這些檔案會觸發後續多階段的感染鏈，最終在遭駭入的系統上部署 Lumma 惡意竊密程式。此惡意軟體的目標是敏感資料，包括密碼、瀏覽器資訊和加密貨幣錢包的詳細資訊。惡意軟體使用先進的迴避技術，例如：利用 Steam 設定檔進行 C&C 作業。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Wmic-Http!g1
- ACM.Wmip-Mshta!g1
- ACM.Wmip-Ps!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：
- CL.Downloader!gen111
- Scr.Heuristic!gen20
- Scr.Mallnk!gen10
- Scr.Malcode!gen
- Scr.Mallnk!gen13
- Trojan.Gen.MBT
- Web.Reputation.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/02/23

流行趨勢是很好的釣餌～偽裝成ChatGPT訂閱通知的網路釣魚行動

在賽門鐵克最近觀察到網路釣魚行動中，偽裝成「每月續訂」通知的電子郵件正大肆傳送給目標收件者。主旨通常包含「action required」(需採取行動) 或「Reminder」(提醒) 等關鍵字，這是引誘收件者開啟電子郵件的常用手法。電子郵件的本文宣稱需要每月支付 24 美元的訂閱費才能使用 ChatGPT 的進階功能。若要完成付款，收件者會被提示點擊一個目的在竊取其憑證的網路釣魚網址。電子郵件標頭如下：

- Subject：Action Required: Secure Continued Access to ChatGPT with a $24 Monthly Subscription
  From:ChatGPT <假冒的郵件信箱>。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/02/21

Core勒索軟體--源於Makop的後繼最新變種

Core 勒索軟體是源於 Makop 的後繼最新變種，最近已經出現在真實網路情景上。該勒索軟體會加密使用者檔案，並冠上 .core 副檔名。受害者的編號和開發者的電子郵件地址也會附加到副檔名中。該勒索軟體會以檔名為「README-WARNING.txt」的文字檔形式留下勒索 (贖金支付) 說明。Core 還具有刪除受遭駭端點上的陰影副本和備份資料的功能，以及修改登錄檔機碼取得常駐功能。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：
- Ransom.Makop!g1

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/02/21

Ghost(也稱為Cring)勒索軟體

賽門鐵克的安全機制應變中心 (Symantec Security Response) 得知美國網路安全暨基礎設施安全局 (CISA)、聯邦調查局 (FBI)、各州資訊共享及分析中心 (MS-ISAC) 針對勒索軟體 Ghost (也被叫做 Cring）最新一波攻擊提出警告，指出這些駭客通常會對於提供網際網路服務的應用系統已知漏洞下手，從而入侵並以勒索軟體加密檔案。這個勒索軟體家族的幕後指使者濫用已公開揭露的漏洞，試圖開採提供網際網路服務伺服器的弱點。開採濫用下列 (但不限於) CVE-2018-13379、CVE-2010-2861、CVE-2009-3960、CVE-2021-34473、CVE-2021-34523、CVE-2021-31207 等陳年漏洞。

根據已發佈的警告，Ghost／Cring 勒索軟體至今已入侵超過 70 個國家的各行各業。已部署的勒索軟體有效酬載會加密使用者檔案，隨附的勒索 (贖金支付) 說明有些還會特別註明可能會外洩使用者的機敏資料。攻擊者在攻擊中使用 Cobalt Strike 和許多開放原始碼工具，包括 IOX、SharpZeroLogon、BadPotato 等。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Ps-Net!g1
- ACM.Ps-Sc!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：
- AGR.Terminate!g2
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.TCP!gen1
- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：
- Hacktool.Iox
- PUA.Gen.2
- Ransom.Gen
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：
- Web Attack: ColdFusion Remote Code Exec CVE-2010-2861
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473

2025/02/21

喬裝成xigncode反作弊程式的惡意程式有XWorm惡意程式的特質

最近，有人發現偽裝成 xigncode 反作弊程式的可執行檔的惡意軟體樣本。XingCode 是線上遊戲常用的反作弊軟體，用來防止作弊、駭客入侵和未經授權的第三方工具。這些惡意檔案包含內嵌的 PowerShell 腳本，用於對資料進行去混淆處理。這些檔案展現出 XWorm 惡意軟體的特質，具有系統操控、資料外洩和鍵盤記錄等功能，意在建立常駐／持久性和逃避偵測。

XWorm 是一種基於 .NET 的商品化遠端存取木馬 (RAT)，在真實網路情境被廣泛操弄。雖然該惡意軟體家族在過去曾多次被發現，但新版本仍在地下論壇上出售，並可能由不同的威脅組織在不同的攻擊行動中大肆傳播。除了典型 RAT 常見的功能外，XWorm 最新變種還具有一些額外的竊密功能，允許攻擊者收集機密的使用者資料、銀行詳細資訊、憑證、cookie 和其他資訊。該惡意軟體還可以從 C&C 伺服器下載其他外掛程式，從而進一步增強其運作能力。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Ps-RgPst!g1
- ACM.Untrst-Schtsk!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-FlPst!g1

基於行為偵測技術(SONAR)的防護：
- SONAR.Dropper
- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen752

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：
- ISB.Heuristic!gen5
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.SecurityRisk.4

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/02/20

散播Rhadamanthys惡意竊密程式的攻擊行動濫用Microsoft管理控制台(MSC)檔及操作視窗被用來傳播惡意軟體

自 2024 年年中以來，MSC 惡意軟體涉入的惡意行動日益增多，並發現有人濫用 CVE-2024-43572 Microsoft Windows Management Console 遠端程式碼執行 (RCE) 漏洞進行攻擊。已觀察到一個散佈 Rhadamanthys 惡意竊密程式的攻擊行動，該惡意軟體偽裝成 MSC 檔案。新發現的 MSC 檔案屬於透過 Console Taskpad 執行「command」指令的惡意程式。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Ps-CPE!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：
- SONAR.SuspStart!gen14

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：
- Web Attack: Microsoft Management Console CVE-2024-43572 Download

2025/02/20

奈及利亞威脅份子散佈XLogger惡意軟體

奈及利亞威脅份子的惡意軟體攻擊行動已被觀察到散佈 XLogger 惡意軟體。此行動始於使用 Google dorking 伎倆收集電子郵件位址，並建置偽造的網站在不法業者所提供防彈代管服務上。使用者會被透過 ChatGPT 製作的釣魚電子郵件誘騙，其中包含可執行檔案的 RAR 壓縮附件。執行後，PowerShell 指令碼會解密惡意軟體的有效籌載，用將竊取的資料滲出到 Telegram 頻道。

網路上知識：

谷歌駭侵法 (Google hacking)，也叫 Google dorking，是一種利用谷歌搜尋和其他谷歌應用程式來發現網站配置和程式碼中的安全漏洞之駭客伎倆。

防彈代管 (bulletproof hosting)，泛指網站服務業者所提供主機位於司法比較不嚴謹的地區，執法與查核有相當的困難度，這種服務特別受到非法服務的喜愛。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：
- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：
- Packed.NSISPacker!g19
- Scr.Malcode!gen
- WS.SecurityRisk.4

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

Symantec
A Division of Broadcom

關於賽門鐵克 (Symantec)

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，近三年 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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

關於保安資訊 www.savetime.com.tw

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 年起就全心全力專注在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，以及基於比原廠更熟悉用戶使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。