思科
2017 年度網路安全報告

cisco

目錄

綜合摘要

隨著攻擊面增加，防禦者必須專注於最重要的目標：減少惡意人士的操作空間。

惡意人士可用的工具超出以往，（惡意人士比以往擁有更多的工具）更可以準確的在最佳時機利用每個工具，使其發揮最大效用。行動通訊應用和線上流量的爆炸性成長更助長其態勢。他們擁有更大的操作空間和更多可選擇的目標及手法。

防禦者可以利用一系列的策略，以因應不斷擴大的威脅及挑戰。此外，他們可以分別購買各種品牌最佳解決方案，並各自獨立運作以提供資訊和保護，必須在人才短缺且預算吃緊的市場中，爭取到適合的專業人員。

停止所有資安攻擊，似乎不太可能。但您可以限制惡意人士的操作空間，進一步限制其危害資產的能力，才能將風險和威脅的影響降到最低。您可以採取的措施是將資安工具統合並簡化，並可以相互關聯及整合在安全性架構中。

在自動化架構中搭配運作的整合式資安工具可簡化偵測的過程和減輕威脅。如此，您便能有時間解決更複雜且持續存在的問題。許多組織至少會使用六種解決方案，而這些解決方案也可能皆來自不同廠商（第 53 頁）。在許多情況下，資安團隊只能調查在當天收到的所有資安警示一半的量。

思科 2017 年度網路安全報告呈現由思科安全研究部門提供的研究、深入分析和觀點。我們不僅會強調在惡意人士嘗試取得更多操作時間，與防禦者努力關閉攻擊者試圖利用機會當中所呈現的拉鋸狀態，還會考察思科威脅研究人員及其他專家彙編的資料。我們的研究和見解目的在協助組織有效應變現今快速變化且複雜的威脅。

本報告分為以下各節：

攻擊者行為

在本節中，我們會分析攻擊者如何偵測脆弱的網路並傳送惡意軟體；也說明如何將電子郵件、第三方雲端應用程式和廣告軟體等工具武器化；還會說明網路罪犯利用安裝階段中所運用的攻擊方法。本節也會介紹我們的「Time to evolve」(TTE) 研究，說明惡意人士如何維持最新的戰術和規避偵測。我們也會提供盡力減少平均偵測用時 (TTD) 的最新消息。此外，還會提供思科針對各產業和地理區域的惡意軟體風險所進行的最新研究。

防禦者行為

我們會在本節中說明最新漏洞的相關消息，而其中一項重點擺在中介軟體程式庫浮現的弱點，這使得惡意人士有機會利用相同的工具入侵多種應用程式，如此會減少入侵使用者時所需的時間與成本。除此之外，我們也會分享思科對於修補程式趨勢的研究。我們發現讓使用者定期更新的好處是，可以鼓勵他們採用更安全的一般網頁瀏覽器版本和生產力解決方案。

思科 2017 年資安能力基準研究

本節涵蓋第三次資安能力基準研究的結果，其內容側重資安專業人員對所屬組織中資安狀態的看法。今年資安專業人員似乎對其現有的工具深具信心，但他們不確定這些資源是否能有助於減少惡意人士的操作空間。該研究也顯示，公共資安漏洞會對商機、營收和客戶產生重大影響同時也會促進組織改良技術和程序。如需更多在組織中資安現況的相關深入分析，請前往第 49 頁。

產業

在本節中，我們將說明確保價值鏈安全性的重要性，並且檢視政府單位儲存了廠商產品中具有零時差漏洞攻擊和弱點潛在危害的相關資訊。此外，我們也會探討在快速變動的環境中，如何使用快速加密作為保護資料的解決方案。最後，我們將概述在全球網際網路流量和潛在攻擊面日趨成長與擴張的情況下，組織資安所面臨的各項挑戰。

結論

在結論中，我們建議防禦者確實執行資安規範，以妥善因應攻擊鏈上的典型的資安威脅，並減少惡意人士的操作空間。本節也提供建立整合且簡化資安方法的特定指南，將領導階層、政策、通訊協定和工具相互連結，以便防止、偵測和減輕各種威脅。

主要發現

- Angler、Nuclear 和 Neutrino 等三個主要攻擊套件在 2016 年突然從威脅情勢中消失，留下次要和新型威脅闖出名堂的空間。
- 根據思科 2017 年資安能力基準研究顯示，大多數的公司在其環境中會使用五個以上的資安廠商和五個以上的資安產品。55% 的資安人員至少會使用六家廠商；45% 使用一到五家廠商；65% 使用六個（含）以上的產品。
- 根據此基準研究顯示，採用進階資安產品和解決方案的主要限制是預算（35% 的受訪者表示）、產品相容性 (28%)、認證 (25%) 和人才 (25%)。
- 思科 2017 年資安能力基準研究發現，組織因礙於各項限制只能在當日調查 56% 收到的資安警示。有一半已調查的警示 (28%) 視為有效的警示，而只有不到一半 (46%) 的有效警示經過修復。此外，44% 的資安作業管理員每天都會看到超過 5000 個資安警示。
- 在 2016 年，27% 企業引進雲端應用已造成了高度資安風險。在使用者授與存取權後，開放驗證 (OAuth) 連線會觸及公司基礎架構，並可與企業雲端和軟體即服務 (SaaS) 平台之間自由通訊。
- 思科對垂直市場中 130 個組織所進行的調查發現，75% 的公司都會受到廣告軟體感染的影響。惡意人士會使用這些感染發動其他惡意軟體攻擊。
- 惡意廣告活動背後的操控者越來越多使用Broker（也稱為「閘道」）。Broker可讓惡意廣告活動更快速地移動、維持操作空間和規避偵測。這些中間連結還可允許惡意人士在惡意伺服器之間迅速切換，無需變更原本的重新導向機制。
- 垃圾郵件帳戶佔了將近三分之二 (65%) 的電子郵件總量，而我們的研究顯示，全球垃圾郵件總量正因傳送垃圾郵件的殭屍網路如雨後春筍般地出現而持續成長。思科威脅研究人員表示，於 2016 年觀察到的全球垃圾郵件約有 8% 到 10% 可分類為惡意郵件。此外，夾帶惡意電子郵件附件的垃圾郵件百分比正持續增加，而惡意人士似乎會嘗試各種檔案類型來協助其威脅活動順利進行。
- 根據資安能力基準研究，尚未發生資安漏洞的組織可能自認為自己的網路安全無虞。考慮到 49% 的受訪資安專業人員表示發生資安漏洞後，其組織必須管理公共審查，因此對網路安全可能寄予太大的信心。

- 思科 2017 年資安能力基準研究也發現，有將近四分之一的組織都曾受到攻擊而錯失商機，且 40% 的組織表示這讓他們損失慘重。五分之一的組織曾因攻擊而流失客戶，且近 30% 的組織受到虧損。
- 根據此基準研究的受訪者表示，發生漏洞時，營運和財務是最可能受到影響的企業功能（分別佔 36% 和 30%），接著是品牌信譽和客戶保留率（皆為 26%）。
- 資安漏洞所導致的網路中斷通常會產生深遠的影響。根據此基準研究顯示，45% 的網路中斷會持續 1 到 8 小時、15% 持續 9 到 16 小時，而 11% 則會持續 17 到 24 小時。41%（請參閱第 55 頁）的網路中斷會影響11% 到 30% 的系統。
- 中介軟體的弱點（軟體作為平台或應用程式之間的橋樑或連接器）日益明顯，因而產生中介軟體是否成為常見威脅媒介的疑慮。許多企業依賴中介軟體，因此這項威脅可能會影響每個產業。在 Cisco® 專案期間，我們的威脅研究人員發現大多數檢視到的新弱點是因為使用了中介軟體。
- 提到安裝修補程式和升級，軟體更新的步調會影響使用者行為。根據我們的研究人員表示，定期且可預測的更新排程可讓使用者更快升級軟體，並縮短惡意人士可利用弱點的時間。
- 2017 年資安能力基準研究發現大多數組織至少有 20% 的資安依賴第三方廠商，而非常依賴這些資源的組織最有可能在未來擴充其使用範圍。

簡介

簡介

惡意人士擁有各式各樣的技術組合，可取得組織資源的存取權和不受限制的操作時間。他們的策略不僅涵蓋所有基礎，還包括：

- 利用修補和更新程式之間的間隔時間
- 引誘使用者落入社交工程陷阱
- 植入惡意軟體在合法的線上內容，例如廣告

他們還有具備許多其他能力，不論是入侵中介軟體弱點，還是投下惡意垃圾郵件。一旦達成目標後，便會迅速暗中結束操作。

惡意人士馬不停蹄，持續演進威脅、加快移動速度，並尋找可擴展操作空間的方式。主要由於行動上網的速度加快和線上裝置的普及，網際網路流量因而爆炸性成長，這卻成了他們發展攻擊面的助力。在此情況下，企業的風險也隨之增加。思科 2017 年資安能力基準研究發現，超過三分之一的組織曾因攻擊而損失 20% 或以上的營收。49% 的受訪者表示他們的企業因資安漏洞而曾面臨公開審查。

有多少企業能夠承受此類損害，在挑戰他們的底線之餘還能維持營運上的健全？防禦者必須側重其資源，著重在減少惡意人士的操作空間。接著，攻擊者便會發現要存取寶貴的企業資源，並在不受到偵測的情況下進行活動，可說是極為困難。

自動化是達到此一目標的關鍵，此一方法可協助您瞭解網路環境中的正常活動，讓您將稀有資源放在調查和解決真正的威脅。簡化資安作業也能協助您有效消除惡意人士不受限制的操作空間。但是，基準研究顯示大多數組織正在使用由超過五家廠商所提供的超過五種解決方案（第 53 頁）。

此類複雜的網路技術和數量龐大的資安警示，可提供效果較為有限的保護。聘用更多資安人才一定有所幫助。依照邏輯而言，聘用更多專家，組織便更有能力提升管理技術和產出更好的結果。但是稀有的資安人才和有限的資安預算，卻讓擴大徵才的舉動顯得不切實際。大多數的組織還是只能將就於其擁有的人才，並依賴委外人才增加資安團隊的戰力，同時節省預算。

因應這些挑戰的真正答案，便是透過整合的方式配置人員、程序和技術，這一點我們稍後將於本報告中說明。落實資訊安全，您必須確實瞭解企業需要保護的是什麼，以及應該用於保護這些重要資產的措施。

思科 2017 年度網路安全報告內含最新的資安產業成就介紹，有助於組織和使用者抵禦各項攻擊。此外，我們亦探討惡意人士突破防禦機制的手法和策略。本報告同時列出思科 2017 年資安能力基準研究的重要發現，探討企業的安全性態勢，以及他們對自身備戰程度的認知。

攻擊面擴展

攻擊面擴展

*行動裝置。公共雲。雲端基礎架構。使用者行為。*參與思科第三年度資安能力基準研究的資安專業人員，基於組織風險暴露於網路攻擊的考量，會將上述所有要素視為主要的疑慮來源（圖 1）。這並不難以理解：行動裝置的普及創造了更多需要保護端點。雲端應用正使得安全邊界被延伸。使用者一如往常，仍是安全鏈中最脆弱的一環。

隨著企業採納數位化，物聯網 (IoE)[1] 也開始成形，防禦者需要擔憂的事情也會隨之增加。攻擊面只會進一步擴展，讓攻擊者擁有更多的操作空間。

過去十多年以來，Cisco® 視覺網路指標 (VNI) 已提供全球 IP 流量預測，並分析促進網路成長的動態因素。請考量下列最新報告*皆位元組時代：趨勢與分析*[2] 的統計資料：

- 年度全球 IP 流量將於 2016 年底通過ZetteaByte 的門檻，並在 2020 年達到每年 2.3 ZB。（ZB為 1000 Exabyte，即 10 億兆位元組）。這代表全球 IP 流量在未來 5 年內會增加三倍。
- 到了 2020 年，無線和行動裝置的流量將佔三分之二 (66%) 的 IP 總流量，而有線裝置僅佔 34%。
- 從 2015 年到 2020 年，平均寬頻速度會提升近一倍。
- 到了 2020 年，82% 的所有全球消費型網際網路流量將會是 IP 視訊流量，超越 2015 年的 70%。

圖 1 資安專業人員最為擔憂的網路攻擊來源

行動裝置	公有雲中的資料	雲端基礎架構	使用者行為（如點擊電子郵件或網站中的惡意連結）
58%	57%	57%	57%

認為這些類別非常或極度具挑戰性的資安專業人員的百分比

資料來源：思科 2017 年資安能力基準研究

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

[1] 物聯網常見問題集（思科）：http://ioeassessment.cisco.com/learn/ioe-faq。
[2] *皆位元組時代：趨勢與分析*（思科 VNI，2016 年）：http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html。

此外，思科 *VNI™ 預測與研究方法（2015 至 2020 年）*白皮書[3] 預測 2020 年全球網際網路流量將是 2005 年的 95 倍。

當然，投機取巧的網路罪犯也會密切注意這些趨勢。我們已觀察到在不斷變化環境中，影子經濟的操控者已採取行動讓自己更為敏捷，並創造高度目標導向的各種攻擊，專為成功擴展攻擊面而設計。於此同時，安全性團隊仍持續處於疲於應付警示的滅火模式，他們必須在網路環境中依賴一系列的資安產品，但此舉只會徒增複雜性，甚至增加組織對威脅的敏感性。

組織必須：

- 整合資安技術
- 簡化資安作業
- 更為依賴自動化

此方法有助於降低營運費用、減輕資安人員的負擔，並提供更佳的安全性結果。最重要的是，該方法可讓防禦者將更多時間專注於消除惡意人士目前不受限制的操作空間。

[3] *思科 VNI 預測與研究方法（2015 至 2020 年）*（思科 VNI，2016 年）：
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html。

攻擊者行為

攻擊者行為

偵察 | 武器化 | 派送 | 安裝

攻擊者研究、識別並選擇目標。

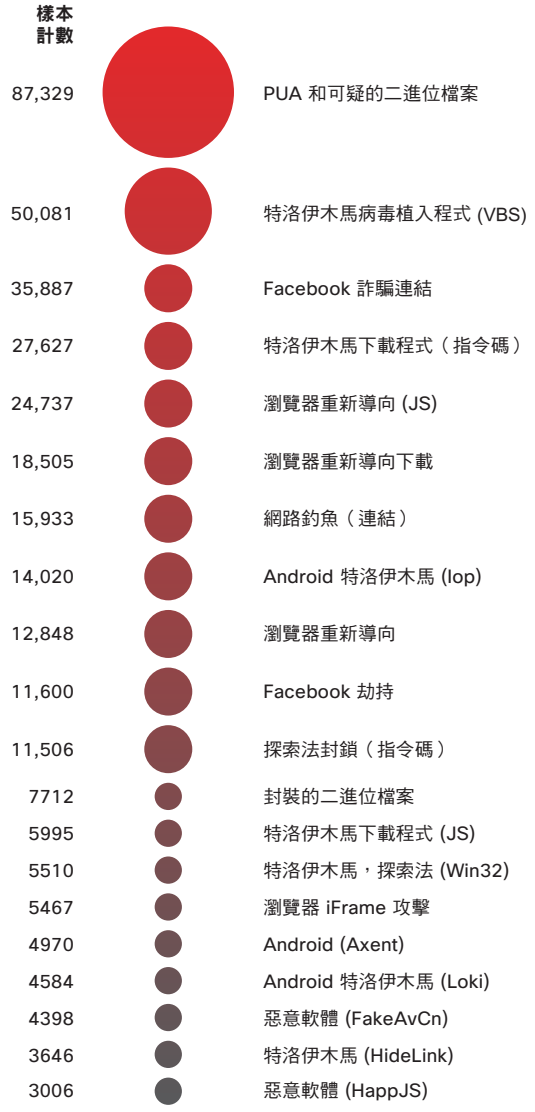
網路攻擊方法：「短尾」威脅有助於惡意人士為威脅活動立下根基

偵察當然是發動網路攻擊的基礎步驟。在此階段中，惡意人士會尋找容易受到攻擊的網際網路基礎架構或網路弱點，讓其存取使用者電腦並最終滲透組織。

可疑的 Windows 二進位檔案和可能不必要的應用程式 (PUA) 以顯著的差異在 2016 年網路攻擊方法清單中位居第一（**請參閱圖 2**）。可疑的 Windows 二進位檔案會傳送間諜軟體和廣告軟體等威脅。惡意的瀏覽器擴充功能便是其中一個 PUA 範例。

包括具有調查詐騙之偽造優惠和媒體內容的 Facebook 詐騙在清單中名列第三。Facebook 詐騙在最常偵測到的惡意軟體年度和年中清單中持續名列前矛，突顯社交工程在許多網路攻擊中的基本作用。Facebook 在全球每個月擁有近 18 億的現用使用者。[4] 這卻讓網路罪犯及其他不肖分子合理詐騙使用者的天地。好消息是該公司最近宣佈其正在採取行動以消除偽造消息和騙局。評論家表示此類內容可能已影響 2016 年美國總統大選的投票者。[5]

圖 2 最常偵測到的惡意軟體



資料來源：思科資安研究部門

[4] Facebook 統計資料（2016 年 9 月）：http://newsroom.fb.com/company-info/。

[5] 祖克柏誓言剷除 Facebook 的「造假新聞」（Jessica Guynn 和 Kevin McCoy，*USA Today*，2016 年 9 月 14 日）：http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/。

瀏覽器重新導向惡意軟體在 2016 年最常觀察到的惡意軟體類型中名列第五。如*思科 2016 年中網路安全報告*[6] 所述，瀏覽器感染會讓使用者暴露於惡意廣告之中，惡意人士會將其用於設定勒索軟體及其他惡意軟體活動。思科威脅研究人員警告表示惡意廣告軟體（包括廣告載入程式、瀏覽器設定綁架程式、公用程式和下載程式）是成長中的問題。事實上，在我們對廣告軟體問題所進行的研究中，已在最近調查公司的 75% 中識別廣告軟體感染。（如需有關此主題的更多資訊，請參閱第 23 頁的「調查發現 75% 的組織都會受到廣告軟體感染的影響」）。

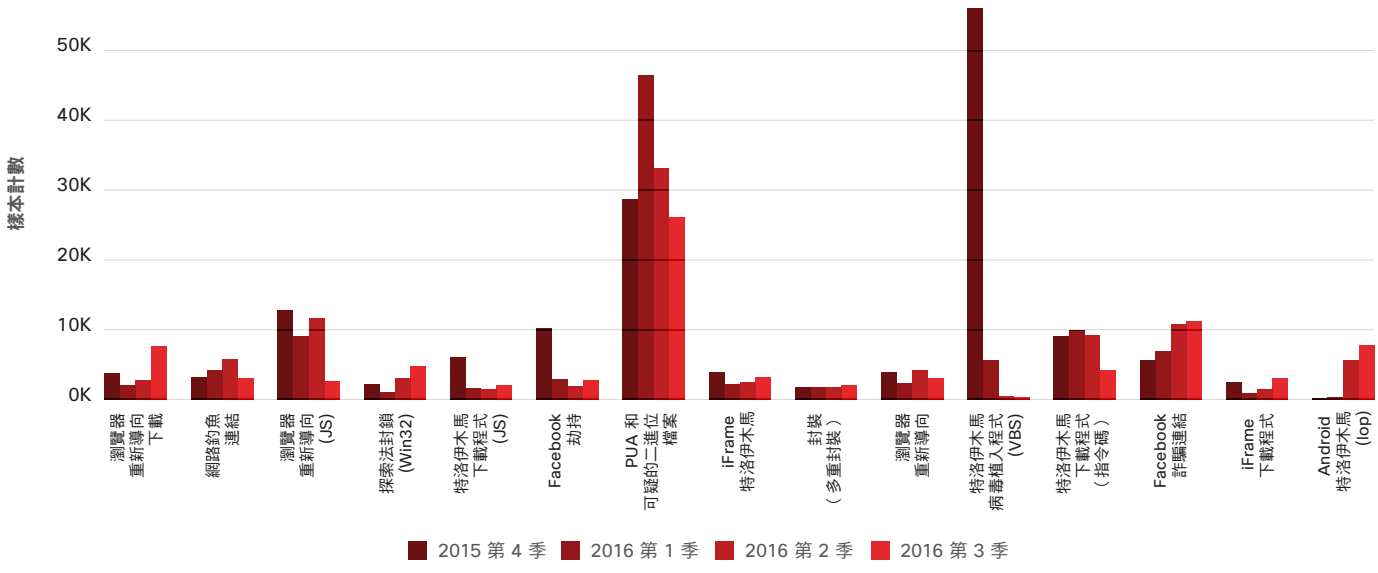
圖 3 所列的其他惡意軟體類型（例如瀏覽器 JavaScript 濫用惡意軟體和瀏覽器 iFrame 濫用惡意軟體）也是專為促進瀏覽器感染而設計。木馬（病毒植入程式和下載程式）也是最常偵測到的惡意軟體類型前五名，表示其仍是一開始存取使用者電腦和組織網路的常見工具。

一貫大量使用以 Android 作業平台使用者為目標的惡意軟體是您需要觀注的另一項趨勢。過去 2 年 Android 木馬的排名已在短尾清單中穩定提升，並名列 2016 年最常見的惡意軟體類型前 10 名。在圖 2（請參閱上一頁）中名列短尾末端的 Loki 惡意軟體可複製和感染其他檔案和程式，因此是特別麻煩的惡意軟體類型。

圖 3 協助說明思科威脅研究人員從 2015 年底觀察到的惡意軟體趨勢，其顯示惡意人士在網路攻擊的偵察階段中發生明確的轉變。更多威脅現在會特別尋找容易受到攻擊的瀏覽器和外掛程式。這項轉變對應於由於惡意人士越來越難以透過傳統網路攻擊媒介入侵大量使用者，而越來越依賴惡意廣告的情況（請參閱下一節第 15 頁的「網路攻擊媒介：Flash 逐漸淡出，但使用者仍須保持警戒」）。

這已向個別使用者、資安專業人員和企業傳達明確的訊息：確定瀏覽器是否安全和停用或移除不必要的瀏覽器外掛程式有助於防止惡意軟體感染。這些感染會導致更重大、更具破壞性且代價更高昂的攻擊，例如勒索軟體活動。這些簡單步驟可大幅降低您暴露於常見網路威脅的風險，並防止惡意人士找到執行攻擊鏈下一個階段（即武器化）的操作空間。

圖 3 2015 年第四季至 2016 第三季最常偵測到的惡意軟體



資料來源：思科資安研究部門

[6] *思科 2016 年中網路安全報告*：http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html。

偵察 | **武器化** | 派送 | 安裝

攻擊者針對漏洞選擇酬載適當的遠端存取惡意軟體。

網路攻擊媒介：Flash 逐漸淡出，但使用者仍須保持警戒

對要入侵系統的惡意人士而言，Adobe Flash 長期以來都是具有吸引力的網路攻擊媒介。但是，隨著 Adobe Flash 內容數量在網路上持續減少且對 Flash 弱點的警覺性提升，網路罪犯越來越難以他們昔日慣用的規模攻擊使用者。

Adobe 已非具有完整開發和支援的軟體平台，並鼓勵開發人員採用 HTML5 等更新標準。[7] 常見網頁瀏覽器的供應商也佔據著高於 Flash 的強勢地位。例如，Google 在 2016 年宣佈會逐步停止 Chrome 瀏覽器上對 Adobe Flash 的完整支援。[8] Firefox 仍持續支援舊版 Flash 內容，但會封鎖「對使用者經驗非必須的特定 Flash 內容」。[9]

Flash 可能已逐漸淡出，但攻擊套件開發人員仍持續將其視為攻擊媒介。但是，我們已觀察到情況可能會有所改變的跡象。Angler、Nuclear 和 Neutrino 等三個主要攻擊套件在 2016 年突然從威脅領域消失後，我們的威脅研究人員觀察到與 Flash 相關的網際網路流量顯著下降。（請參閱第 20 頁的「主要攻擊套件銷聲匿跡，次要和新型威脅得以出頭」）。Angler 攻擊套件背後的操控者嚴重以 Flash 弱點為目標，以危害使用者；Nuclear 攻擊套件也同樣側重於 Flash；而 Neutrino 則依賴 Flash 檔案傳送攻擊程式。

使用者必須保持謹慎，且除非基於商業原因需要使用 Flash，否則應該將其解除安裝。如果必須使用 Flash，則必須持續更新。使用具有自動修補功能的網頁瀏覽器也會有所助益。如第 13 頁的「網路攻擊方法：『短尾』威脅有助於惡意人士為威脅活動立下根基」所述，使用安全的瀏覽器和停用或移除不必要的瀏覽器外掛程式會大幅降低您暴露於網路威脅的風險。

Java、PDF 和 Silverlight

Java 和 PDF 的網際網路流量在 2016 年均已大幅減少。Silverlight 流量已達到不值得威脅研究人員定期追蹤的層度。

曾是主要網路攻擊媒介的 Java 在最近幾年的安全性態勢已大幅改善。Oracle 在 2016 年初決定淘汰其 Java 瀏覽器外掛程式，以降低 Java 淪為網路攻擊媒介的機會。PDF 攻擊也越來越罕見，因此使用者可更輕鬆地偵測到這些攻擊，這也讓惡意人士現在較少使用此策略。

但是，與 Flash 一樣，網路罪犯仍會使用 Java、PDF 和 Silverlight 入侵使用者。個別使用者、企業和資安專業人員必須注意這些潛在入侵途徑。若要降低暴露於這些威脅的風險，則必須：

- 下載修補程式
- 使用最新的網路技術
- 避免可能存在風險的網路內容

[7] Flash、HTML5 和開放網頁標準（Adobe News，2015 年 11 月）：https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html。
[8] Flash 與 Chrome（Anthony LaForge，The Keyword 部落格，Google，2016 年 8 月 9 日）：https://blog.google/products/chrome/flash-and-chrome/。
[9] 減少 Firefox 中的 Adobe Flash 用量（Benjamin Smedberg，Future Release 部落格，Mozilla，2016 年 7 月 20 日）：https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/。

應用程式安全性：在爆炸性成長的應用程式中管理 OAuth 連線風險

隨著企業移轉至雲端，其安全邊界也延伸至虛擬領域。但是，員工引進環境的每台連線第三方雲端應用程式都讓安全邊界快速消失。

工作者想要在工作中改善生產力並保持連線，但這些影子 IT 應用程式會產生企業風險。一旦使用者透過開放驗證 (OAuth) 授予存取權，這些連線便會觸及公司基礎架構，且可在企業雲端和軟體即服務 (SaaS) 平台之間自由通訊。這些應用程式可能具有廣泛的存取範圍，且有時候可能會過度存取。由於其可檢視、刪除、外部化和儲存企業資料，甚至代表使用者執行動作，因此使用者必須謹慎管理這些應用程式。

雲端安全性供應商 CloudLock 現在已納入思科旗下，其在代表一系列產業的 900 個組織樣本群中，已追蹤連線第三方雲端應用程式的成長情況。如**圖 4** 所示，我們已在 2016 年初觀察到約 129,000 個唯一應用程式。到了 10 月底，該數字已成長至 222,000 個。

從 2014 年以來，應用程式數量已增加約 11 倍（請參閱**圖 5**）。

分類出最危險的應用程式

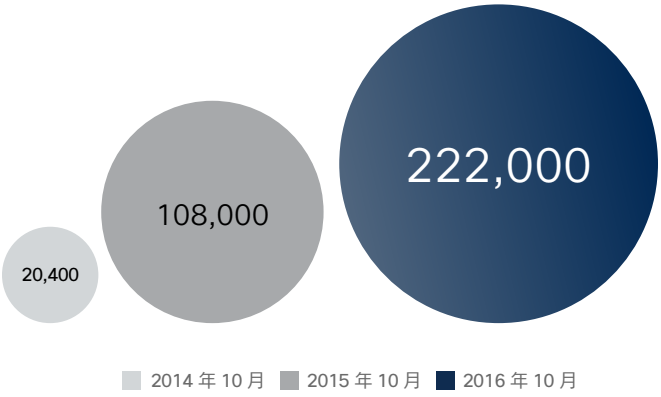
CloudLock 已開發出雲端應用程式風險索引 (CARI)，以協助資安團隊瞭解環境中的哪些連線第三方雲端應用程式會產生最高的網路安全性風險。該程序包含下列數項評估：

- **資料存取需求：**組織會回答下列問題等：授權應用程式所需的權限為何？授予資料存取權是否表示應用程式具有透過 OAuth 連線存取公司 SaaS 平台的程式設計 (API) 存取權？應用程式（或延伸至廠商）是否可代表使用者執行動作，並對公司資料執行動作，例如檢視和刪除？
- **社群信任評分：**此評估使用同業導向和眾包評估。
- **應用程式威脅情報：**由網路安全專家進行全面背景檢查，並以應用程式的各種安全性屬性（例如安全性認證、漏洞記錄和分析人員審核）為基礎。

圖 4 連線第三方雲端應用程式呈現爆炸性成長（2016 年）

資料來源：思科 CloudLock

圖 5 第三方雲端應用程式的成長（逐年比較）



資料來源：思科 CloudLock

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

風險評分與範例

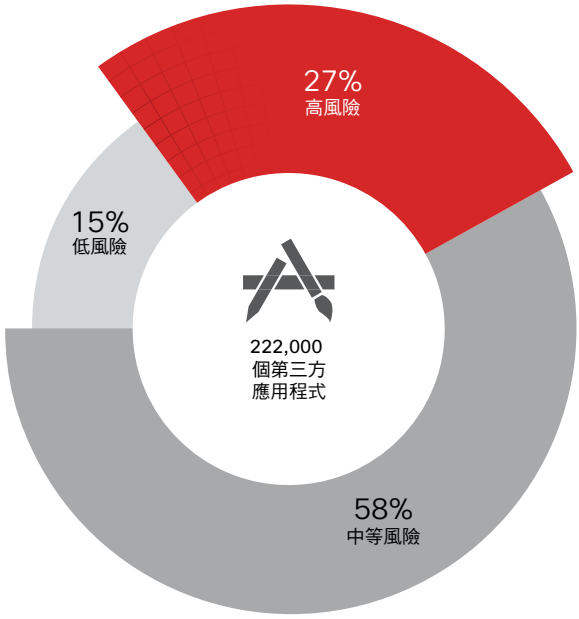
CloudLock 在使用 CARI 分類第三方雲端應用程式後，會針對每個應用程式給予 1 分（最低風險）至 5 分（最高風險）的風險評分。

舉例來說，1 分的應用程式具有範圍最小的存取權（只能查看電子郵件）、100% 的社群信任評比，而且沒有資安漏洞記錄。

5 分的應用程式可能具有完整的帳戶存取權（可以查看所有電子郵件、文件、瀏覽記錄、行事曆等）、8% 的信任評比（表示只受到 8% 管理者的信任），而且沒有安全性認證。

CloudLock 使用 CARI 分類在 900 個組織樣本中識別的 222,000 個應用程式。在所有這些應用程式中，其將 27% 的應用程式視為高風險應用程式，而大多數的應用程式都落在一般風險類別（請參閱圖 6）。這些組織中的一半都擁有與 2016 年夏季發行之熱門遊戲應用程式相關的 OAuth 連線。

圖 6 分類為高度風險的第三方應用程式

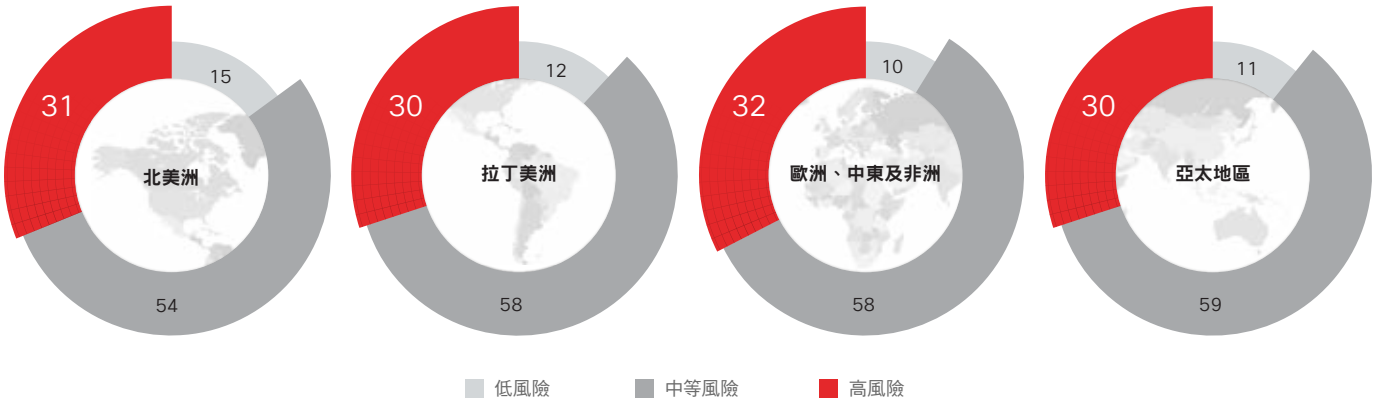


資料來源：思科 CloudLock

分享

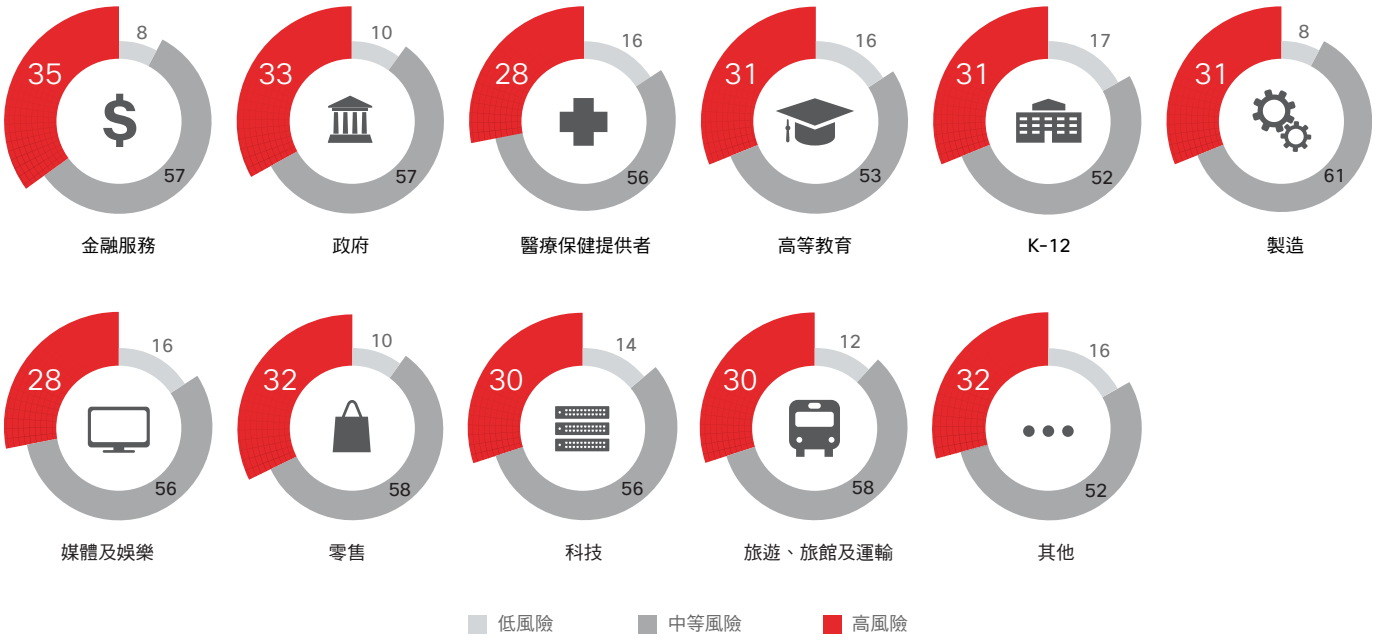
我們透過分析發現無論組織大小、產品或區域為何，所有組織都擁有相對均勻分佈的低風險、一般風險和高風險應用程式（圖 7 和圖 8）。

圖 7 低度、中度和高度風險應用程式的分佈（依區域分類）



資料來源：思科 CloudLock

圖 8 低度、中度和高度風險應用程式的分佈（依產業分類）



資料來源：思科 CloudLock

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

排除雜訊

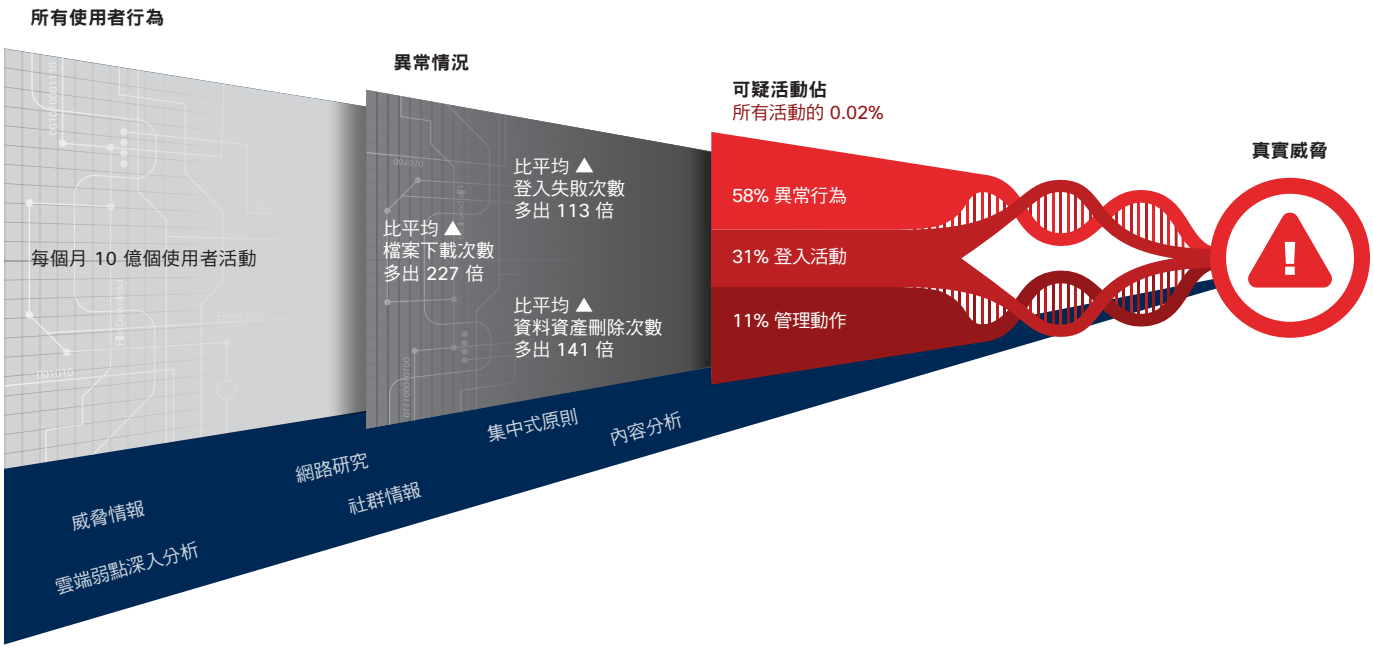
若要識別公司 SaaS 平台中可疑的使用者和實體行為（包括第三方雲端應用程式），安全性團隊必須過濾數十億個使用者活動，以定義組織環境中使用者行為的正常模式，且必須尋找不符合這些預期模式的異常情況，然後建立可疑活動之間的關聯以判斷可能需要進行調查的實際威脅。

在短期內來自許多國家的過度登入活動是其中一個可疑活動範例。假設某個組織中的正常使用者行為是讓員工每週可從不超過一或兩個國家登入特定應用程式。如果使用者在一週內開始從 68 個國家登入該應用程式，資安團隊便會調查該活動以確認其是否合法。

根據我們的分析，與連線第三方雲端應用程式相關的使用者活動中，只有 1/5000 (0.02%) 為可疑活動。資安團隊的挑戰當然是精確定位單一執行個體。

資安團隊只能透過自動化排除資安警示中的「雜訊」，並將資源專注於調查實際威脅。上述可識別正常使用者活動和潛在可疑使用者活動的多階段程序（如圖 9 所說明）關聯就在於透過在所有階段中套件的演算法來使用自動化。

圖 9 透過自動化（程序）識別使用者的行為模式



資料來源：思科 CloudLock

偵察 | 武器化 | **派送** | 安裝

攻擊者惡意使用電子郵件、檔案附件、網站及其他工具，將網路武器傳送至目標。

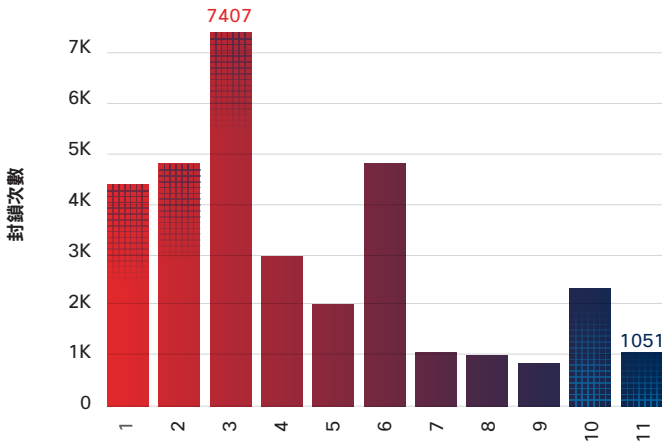
主要攻擊套件銷聲匿跡，次要和新型威脅得以出頭

攻擊套件環境在 2016 年發生劇烈變化。該年年初，Angler、Nuclear、Neutrino 和 RIG 明顯在攻擊套件中遙遙領先。但到了 11 月，這些套件中只剩 RIG 仍然保持活躍。如圖 10 所示，攻擊套件活動約於 6 月時大幅減少。

Nuclear 是第一個消失的攻擊套件，突然於 5 月停止操作。其作者放棄的原因至今仍是一個謎。同樣也在 2016 年黯然退場的 Neutrino 攻擊套件，過去曾仰賴 Flash 檔案來傳送弱點。（如需 2016 年已知攻擊套件中主要弱點清單，請參閱下一頁的圖 11）。

對惡意人士而言，Flash 依然是具有吸引力的網路攻擊媒介，雖然可能隨著時間的消逝而逐漸沒落。幾乎沒有網站和瀏覽器可完整或完全支援 Flash，而且普遍對 Flash 弱點更有所警覺。（如需更多此主題的相關資訊，請參閱第 15 頁「網路攻擊媒介：Flash 逐漸淡出，但使用者仍須保持警戒」。）

圖 10 攻擊套件的登陸頁面封鎖數量（2016 年 1 月至 11 月）



資料來源：思科資安研究部門

下載 2017 年圖表：www.cisco.com/go/acr2017graphics

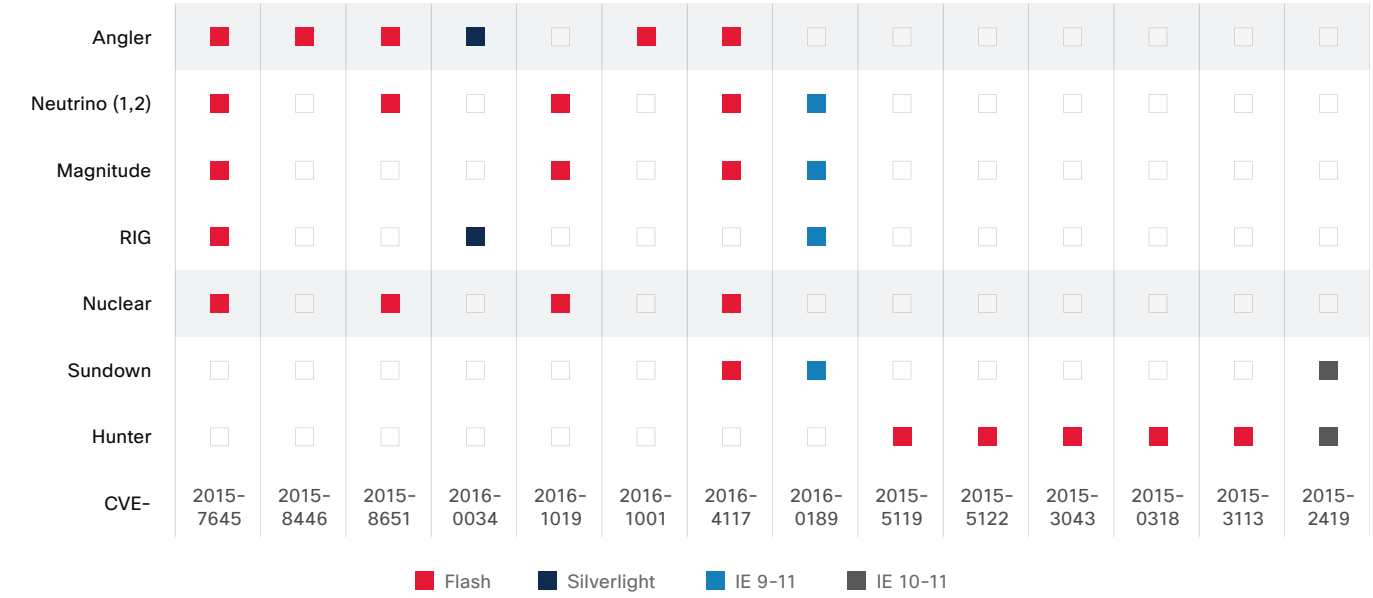
昔日巨頭銷聲匿跡

Angler 是已知攻擊套件中最進階、最大型的一種，也曾以 Flash 弱點為目標，並與許多高能見度的惡意廣告和勒索軟體活動結合。但是，不同於 Nuclear 和 Neutrino 消失的情況，Angler 在 2016 年退場的原因並不神祕。

該年春末，約有 50 位駭客和網路罪犯在俄羅斯遭到逮捕；該集團與 Lurk 惡意軟體有關，那是一種特別針對俄羅斯銀行進行攻擊的銀行木馬。[10] 思科威脅研究人員已識別 Lurk 和 Angler 之間的明確關聯，包括 Lurk 主要透過 Angler 傳送給俄羅斯境內受害者的事實。在拘捕事件發生後，Angler 便從攻擊套件市場上消失。[11]

現在這三種最主要的攻擊套件已退出戰場，次要和新型威脅得以擴展其市場占有率，且變得更加複雜和敏捷。在 2016 年底停滯成長的攻擊套件為 Sundown、Sweet Orange 和 Magnitude。這些套件和 RIG 都是以 Flash、Silverlight 和 Microsoft Internet Explorer 的弱點為目標而聞名。（請參閱圖 11）。解除安裝 Flash 和停用或移除不必要的瀏覽器外掛程式可協助使用者降低遭到這些威脅入侵的風險。

圖 11 攻擊套件的主要弱點



資料來源：思科資安研究部門

分享

[10] 俄國駭客幫派落網，竊取金額超過 2,500 萬元（BBC News，2016 年 6 月 2 日）：http://www.bbc.com/news/technology-36434104。
[11] 如需此主題的詳細資料，請參閱 2016 年 7 月 Cisco Talos 部落格文章：連點成面，揭露犯罪軟體的變化。

惡意廣告：惡意人士利用中介提升速度和靈活度

誘騙使用者前往惡意攻擊套件的管道主要有二：遭駭網站和惡意廣告。惡意人士會將惡意網告或遭駭網站的連結放在惡意攻擊套件的登陸頁面，或是使用一種稱為中介的中間連結。（這種連結位於遭駭網站和惡意攻擊套件伺服器之間，所以又稱為「閘道」。)中介伺服器是初始重新導向和實際惡意軟體之間的中介，可將惡意軟體酬載派送給使用者。

中介這種策略近年來日益猖獗，因為攻擊者發現自己必須加緊腳步，才能維持操作空間並躲過偵測。惡意人士可藉此快速地切換惡意伺服器，過程中無需變更初始的重新導向。由於不需經常修改網站或惡意廣告，就能啟動感染鏈，使得惡意攻擊套件的操作人員可以發動時間更長的攻擊。

ShadowGate：符合成本效益的攻擊活動

現在單靠傳統的網路攻擊向量，已經很難入侵大量的使用者（請參閱第 15 頁），因此惡意人士越來越仰賴惡意廣告，誘騙使用者接觸惡意攻擊套件。我們的威脅研究人員曾將一種近期出現的全球惡意廣告活動稱為「ShadowGate」。這種攻擊活動顯示出，惡意廣告已讓惡意人士有更大的彈性和機會，針對不同地區的使用者進行大規模的目標鎖定。

ShadowGate 擴及的範圍包括流行文化、零售、色情和新聞等網站，可能受影響的使用者已達數百萬之多，遍及北美洲、歐洲、亞太地區和中東地區，這種擴及全球及使用多種語言的能力著實令人震驚。

利用網域掩護的 ShadowGate 最早是在 2015 年初被人發現，有時沒有任何動靜，但會隨機重新啟動，將流量導向至惡意攻擊套件的登陸頁面。ShadowGate 最初只是用來將使用者導向至 Angler 攻擊套件，但在 Angler 於 2016 年夏季消失後，使用者開始被導向至 Neutrino 惡意攻擊套件，而 Neutrino 也在幾個月後消失不見。（如需更多此案例的內容，請參閱第 20 頁「主要攻擊套件銷聲匿跡，次要和新型威脅得以出頭」。）

ShadowGate 雖可檢視大量的網路流量，但僅有小部分的互動會將使用者導向至攻擊套件。惡意廣告絕大多數都是以展示的目的為主，也就是在頁面上刊登，不需要與使用者互動。這樣的線上廣告模式可讓 ShadowGate 的主事者，以更具成本效益的方法操作攻擊活動。

我們開始研究 ShadowGate 後，也和一家大型主機代管公司展開合作，回收惡意人士用來發動攻擊的註冊者帳戶，藉此共同降低威脅。隨後，我們更關閉了所有相關的子網域。

如需 ShadowGate 攻擊活動的詳細資料，請參閱 2016 年 9 月 Cisco Talos 部落格文章：Talos ShadowGate 追擊任務：成功阻撓全球惡意廣告活動。

調查發現 75% 的組織都會受到廣告軟體感染的影響

用於合法目的的廣告軟體是透過重新導向、快顯視窗和廣告置入下載或顯示廣告，並為建立者創造營收的軟體。但是，網路罪犯也會利用廣告軟體，以協助他們增加營收來源。其不但使用惡意廣告軟體透過置入廣告盈利，更將其作為促進其他惡意軟體活動（例如 DNSChanger 惡意軟體）的第一步。惡意廣告軟體會透過軟體套件組合傳送；發行者會透過合法應用程式建立安裝程式，以及許多惡意廣告軟體應用程式。

不肖的操控者會將廣告軟體用於：

- 置入廣告，這可能會造成進一步的感染或暴露於攻擊套件
- 變更瀏覽器和作業系統設定，以減弱安全性
- 破壞防毒軟體或其他資安產品
- 取得主機的完整控制權，以安裝其他惡意軟體
- 透過位置、身分識別、使用的服務和最常造訪的網站追蹤使用者
- 竊取個人資料、認證和基礎架構資訊（例如公司內部銷售頁面）等資訊

為了評估企業廣告軟體問題的範圍，思科威脅研究人員已檢視 80 種不同的廣告軟體變種。我們對垂直市場中約 130 個組織進行調查，時間範圍為 2015 年 11 月到 2016 年 11 月。

我們根據每個元件的主要行為，將廣告軟體分類為四個群組：

- **廣告載入程式：**此廣告軟體通常位於瀏覽器，且可影響所有作業系統。
- **瀏覽器設定綁架程式：**此廣告軟體元件可變更電腦設定以降低瀏覽器安全性。
- **公用程式：**此為成長中的大型廣告軟體類別。公用程式是為使用者提供實用服務的網頁應用程式，例如電腦最佳化。這些應用程式可置入廣告，但其主要目的是說服使用者支付該服務。但是，在許多情況下，公用程式只是一種詐騙手法，且不會為使用者提供任何優勢。
- **下載程式：**此廣告軟體可傳送其他軟體，例如工具列。

我們判斷研究中 75% 的組織都會受到廣告軟體感染的影響。

圖 12 受到廣告軟體感染的組織百分比

資料來源：思科資安研究部門

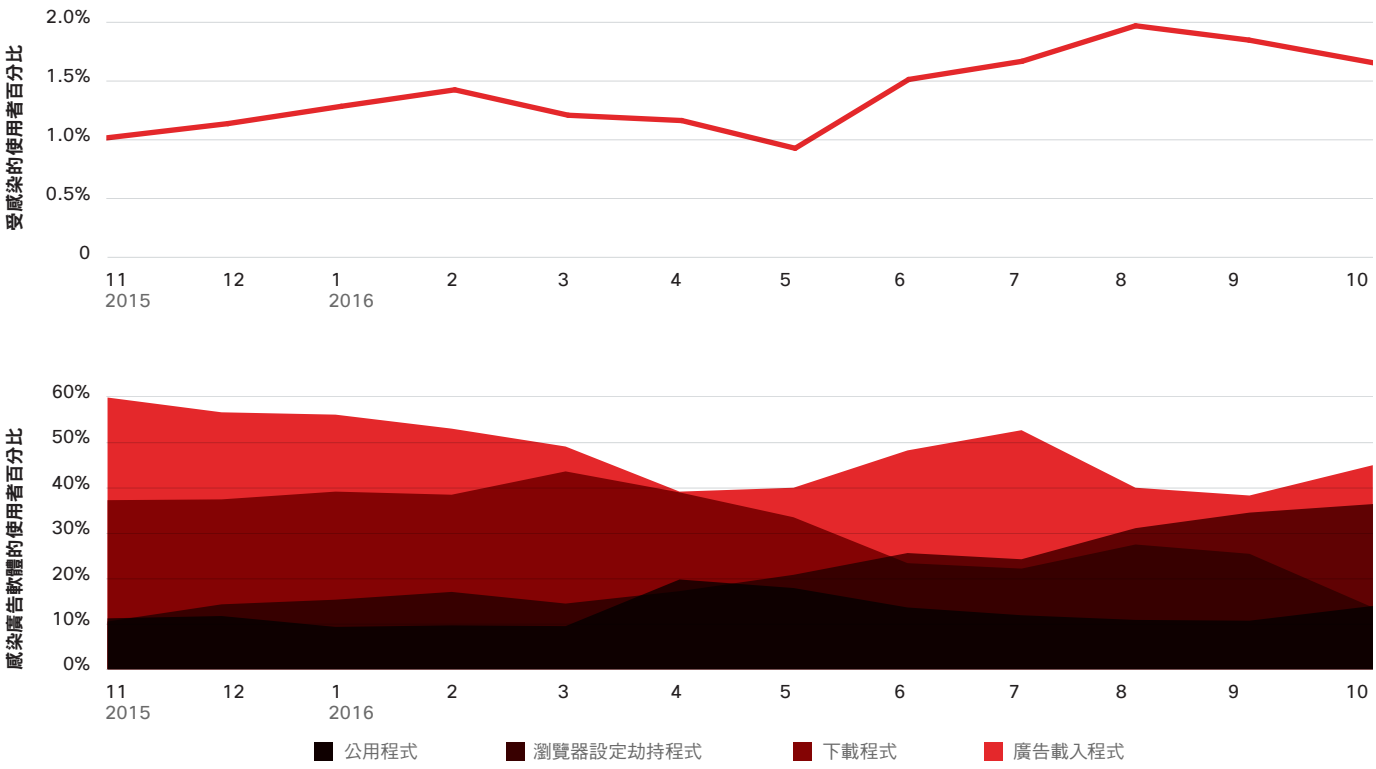
分享

圖 13 顯示我們在調查中的組織觀察到的事件類型。廣告載入程式是主要感染來源。這項發現表示大多數這些不必要的應用程式都會以網頁瀏覽器為目標。我們也在過去幾年內觀察到瀏覽器感染事件的增加，表示惡意人士正在透過此策略嘗試成功入侵使用者。

在我們調查期間識別的所有廣告軟體元件都可讓使用者和組織置身惡意活動的風險之中。資安團隊必須辨識廣告軟體感染導致的威脅，並確保組織中的使用者完全注意到風險。

如需有關此主題的其他資訊，請參閱 2016 年 2 月的思科資安部落格文章與廣告軟體安全基礎相關的 DNSChanger 爆發。

圖 13 依照廣告軟體元件排列的總事件分析



資料來源：思科資安研究部門

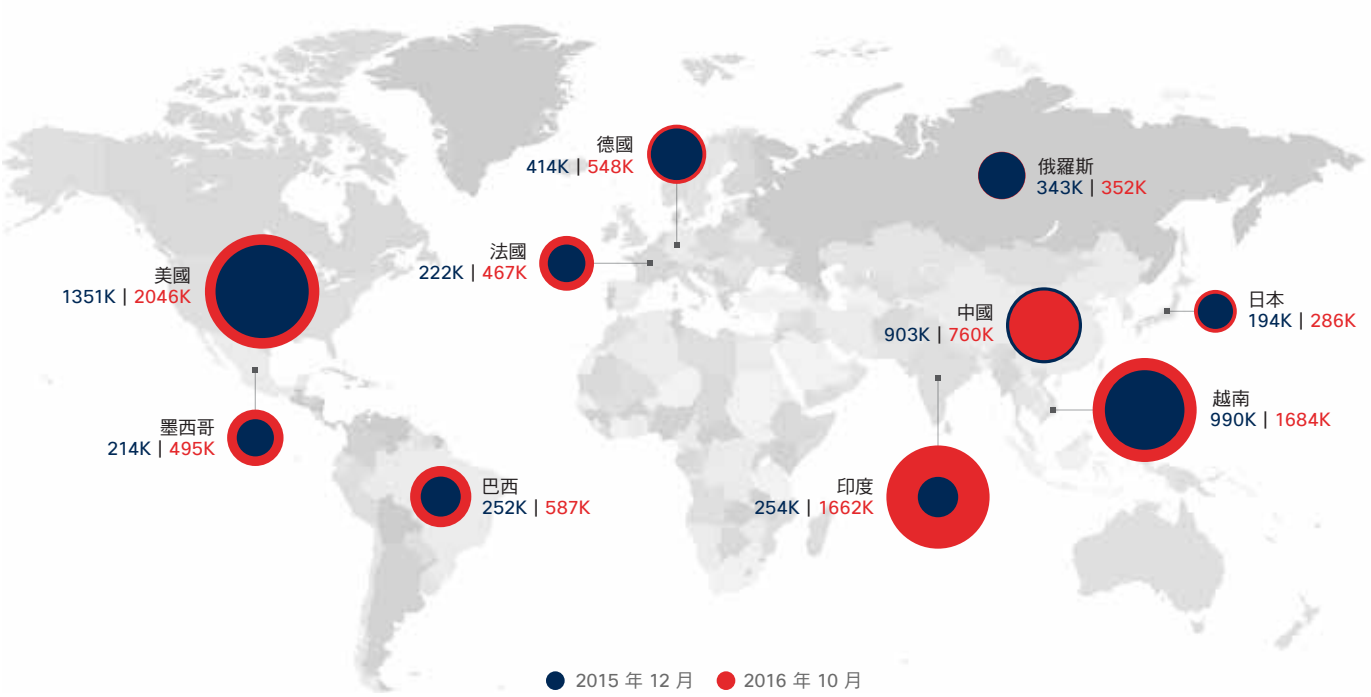
下載 2017 年圖表：www.cisco.com/go/acr2017graphics

全球垃圾郵件和惡意附件百分比正在增加

思科威脅研究人員在 2016 年進行兩項研究使用選擇加入客戶遙測來評估垃圾郵件佔電子郵件總量的百分比。我們發現垃圾郵件帳戶佔據近三分之二 (65%) 的電子郵件總量。我們的研究也表示主要由於 Necurs 等蓬勃發展的大型垃圾郵件傳送殭屍網路，全球垃圾郵件量正在成長。此外，我們也透過分析判斷可將 2016 年約 8% 到 10% 的觀察到的全球垃圾郵件分類為惡意郵件。

從 2016 年 8 月到 10 月，IP 連線封鎖數量已大幅增加（圖 14）。[12] 此趨勢可歸因於垃圾郵件總量增加，以及信譽系統適應有關垃圾郵件傳送者的資訊。

圖 14 各國 IP 封鎖數量（2015 年 12 月至 2016 年 11 月）



資料來源：思科資安研究部門

分享

[12] IP 連線封鎖係指：由於垃圾郵件寄件者的評價分數不佳，而立即遭到垃圾郵件偵測技術封鎖的垃圾郵件訊息，例如：曾經參與垃圾郵件攻擊的已知殭屍網路或遭駭網路傳送的訊息。

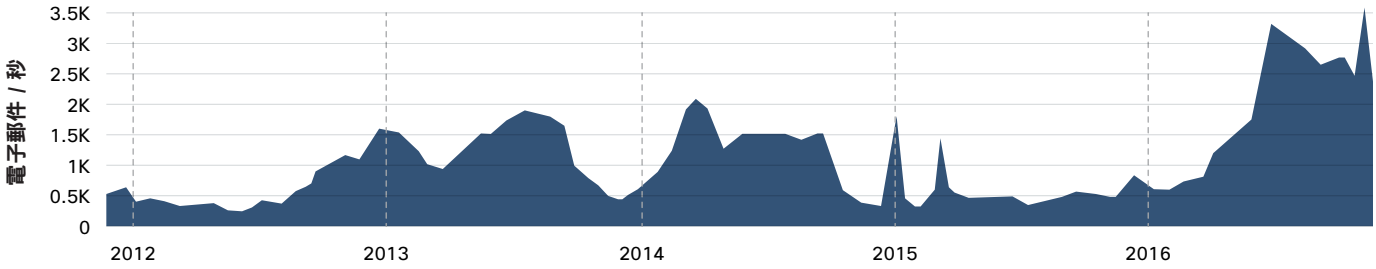
綜合封鎖清單 (CBL) 是可疑的垃圾郵件傳送電腦感染之 DNS「黑洞清單」[13]，其所提供為期五年的圖形也顯示 2016 年垃圾郵件量動態增加（圖 15）。

10 年的 CBL 資料（未顯示）表示 2016 年垃圾郵件量接近 2010 年後觀察到的歷史新高。新的反垃圾郵件技術和知名的垃圾郵件相關殭屍網路斬首行動在最近幾年協助讓垃圾郵件水平保持低檔。我們的威脅研究人員將最近全球垃圾郵件量增加歸因於 Necurs 殭屍網路。Necurs 是 Locky 勒索軟體的主要媒介，也會散佈 Dridex 銀行木馬等威脅。

圖 16 思科 SpamCop 服務產生的內部圖形，說明 2016 年觀察到的垃圾郵件量變化。此圖形顯示 SpamCop 封鎖清單 (SCBL) 從 2015 年 11 月到 2016 年 11 月的整體大小。SCBL 中的每列都代表不同的 IP 位址。

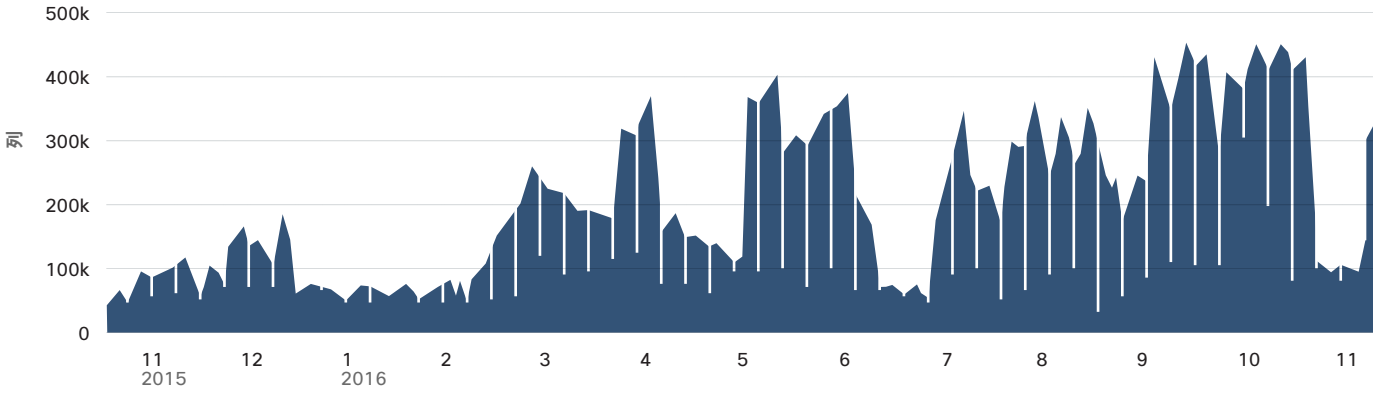
在 2015 年 11 月到 2016 年 2 月之間，SCBL 大小徘徊於 200,000 個 IP 位址以下。SCBL 大小在 10 月減少前，於 9 月和 10 月超過 400,000 個 IP 位址，而我們的威脅研究人員將其歸因於 Necurs 操控者想要抽空休息。另請注意其大小在 6 月時顯著減少的情況。5 月底俄羅斯發生與 Lurk 銀行木馬相關的拘捕事件（請參閱第 21 頁）。隨後，許多知名威脅（包括 Necurs）都就此銷聲匿跡。但是，Necurs 在 3 週後卷土重來，2 小時內在 SCBL 中添加超過 200,000 個 IP 位址。

圖 15 垃圾郵件總數



資料來源：CBL

圖 16 SCBL 總大小



資料來源：SpamCop

分享

[13] 如需 CBL 的詳細資訊，請前往 http://www.abuseat.org/。

許多傳送 Necurs 垃圾郵件的主機 IP 都已遭到感染超過 2 年。為了持續隱藏整個殭屍網路範圍，Necurs 只會從受感染主機的子集傳送垃圾郵件，其可能會持續使用受感染的主機 2 到 3 天，然後有時候會持續 2 到 3 週不使用該主機。此行為讓要因應垃圾郵件攻擊的安全工作人員工作更形複雜。他們可能認為其已找到並成功清除受感染的主機，但 Necurs 後背後的操控者不過是在等待時機發動另一波攻擊。

2016 年 10 月觀察到垃圾郵件總數的 75% 都包含惡意附件，其中大多數的垃圾郵件都是由 Necurs 殭屍網路傳送（請參閱圖 17）。Necurs 會傳送包括內嵌可執行檔（例如 JavaScript、.hta、.wsf 和 VBScript 下載程式）的惡意 .zip 附件。計算包含惡意附件之垃圾郵件總數的百分比後，我們將「包裝好的壓縮檔」檔案 (.zip) 和其中包覆的「子」檔案（例如 JavaScript 檔案）視為個別的惡意附件。

攻擊者嘗試附件類型，讓惡意垃圾郵件活動保持最新狀態

我們的威脅研究人員已檢視惡意人士如何使用不同類型的附件以助於防止惡意垃圾郵件遭到偵測。我們發現其持續演進策略、嘗試各種檔案類型，並在發現活動失敗時快速切換策略。

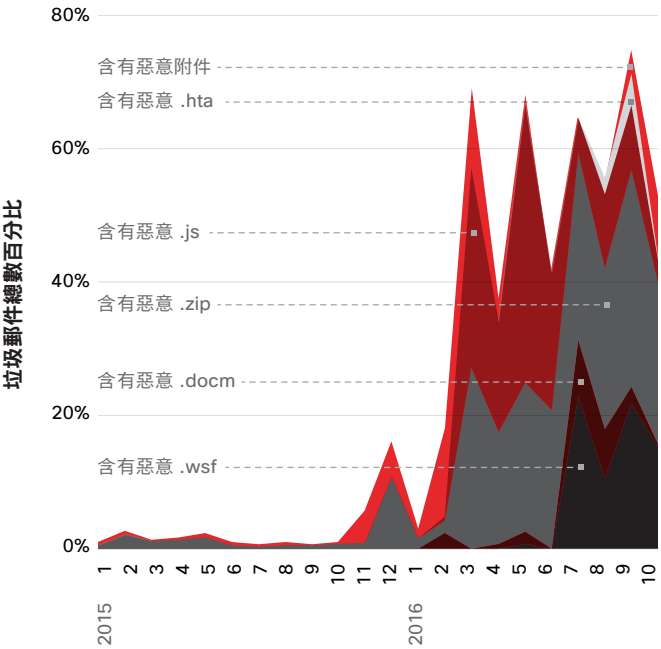
圖 17 顯示惡意垃圾郵件操控者如何在觀察期間內嘗試使用 .docm、JavaScript、.wsf 和 .hta 檔案。如前所述，許多這些檔案類型都與 Necurs 殭屍網路傳送的垃圾郵件相關（如需與其他已檢視檔案類型相關的研究，請參閱第 78 頁的附錄）。

我們使用指定月份中觀察到包含惡意附件之垃圾郵件總數的百分比取得該月不同檔案類型的特定百分比。因此，例如，.docm 檔案在 2016 年 7 月代表觀察到惡意附件總百分比的 8%。

2016 年期間 .wsf 檔案的模式（請參閱圖 17）提供惡意人士如何隨著時間推移，演進惡意垃圾郵件策略的範例。惡意人士在 2016 年 2 月前極少使用此檔案類型作為惡意附件。然後，隨著 Necurs 殭屍網路逐漸活躍，使用此檔案類型的情況開始成長。到了 7 月，.wsf 檔案已佔據所有惡意垃圾郵件附件的 22%。全球垃圾郵件活動也約在此時大幅增加（請參閱上一節），主要由於 Necurs 殭屍網路而有所增加。

經過 8 月、9 月和 10 月，我們觀察到 .wsf 檔案百分比有所波動。這表示檔案類型經常遭到偵測時，惡意人士不時暫時撤退。

圖 17 所有垃圾郵件含有惡意附件的百分比



資料來源：思科資安研究部門

Hailstorm 和 Snowshoe

Hailstorm 攻擊和 Snowshoe 攻擊等兩種類型的惡意垃圾郵件攻擊特別會對防禦者造成問題。這兩種類型都採用速度和目標性元素，且都非常有效。

Hailstorm 攻擊以反垃圾郵件系統為目標。這些攻擊背後的操控者會利用發動垃圾郵件活動和反垃圾郵件系統觀察到活動之間非常短的時間窗口，將範圍延伸至反垃圾郵件掃描器以外的部分。在活動遭到偵測和封鎖前，惡意人士通常只有幾秒或幾分鐘的時間進行活動。

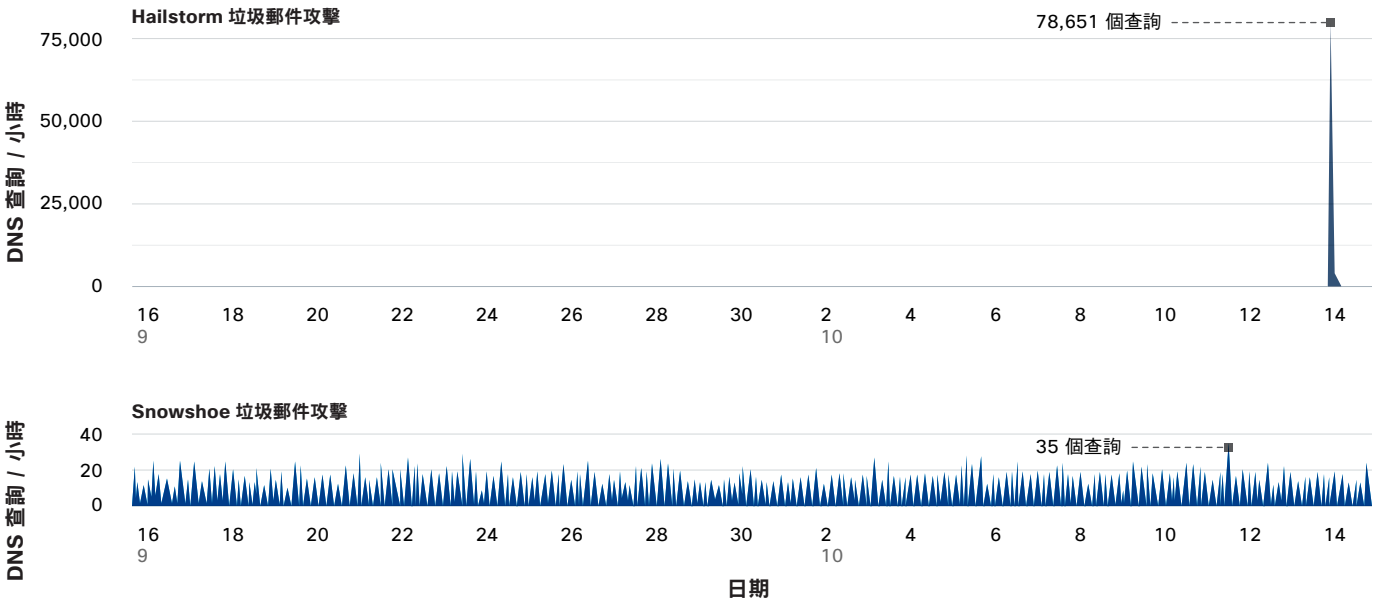
圖 18 中的峰值便是 Hailstorm 攻擊。該活動顯示於思科調查介面。在攻擊前，沒有人在解析 IP 位址。然後，解析 DNS 網域的電腦數量突然攀升至超過 78,000 台，最後再跌落回到零台。

相較於 Hailstorm 攻擊，Snowshoe 垃圾郵件活動也顯示於圖 18，其中攻擊者會嘗試低調規避流量式偵測解決方案。DNS 查詢數量非常穩定，但每小時只有約 25 個查詢。這些低量攻擊可讓惡意人士從廣泛的 IP 位址範圍中，暗中散佈垃圾郵件。

即使這些垃圾郵件攻擊以不同方式活動，其仍具有共同點。透過任何一種方法，惡意人士可以：

- 從未受感染的 IP 和網域傳送以規避不良信譽
- 透過專業內容和訂閱管理的模仿行銷郵件
- 使用正確設定的電子郵件系統，而非草率的指令碼或垃圾郵件 Bot
- 正確設定轉送確認的反向 DNS 和傳送政策架構 (SPF) 記錄

圖 18 Hailstorm 和 snowshoe 垃圾郵件攻擊的比較



資料來源：思科調查

分享

惡意人士也可透過文字變異和循環檔案類型，削弱內容偵測（如需網路罪犯如何演進威脅以規避防禦者的詳細資訊，請參閱第 34 頁的「演進時機」一節）。如需有關其如何針對垃圾郵件嘗試使用惡意檔案附件的更多資訊，請參閱上一節。

圖 19 顯示最常見的威脅爆發警示；此為我們觀察到惡意人士在 2016 年經常更新以略過電子郵件安全性檢查和規則的垃圾郵件和網路釣魚訊息概觀。請務必瞭解哪些類型的電子郵件威脅最常見，以避免遭到這些惡意訊息詐騙。

圖 19 最常見的威脅爆發警示

版本	發佈識別碼	發佈名稱和 URL	訊息摘要	附件的檔案類型	語言	上次發佈日期
96	35656	RuleID4626	發票、付款	.zip	德文、英文	2016/04/25
87	34577	RuleID10277	採購單	.zip	德文、英文	2016/06/02
82	36916	RuleID4400KVR	採購單	.zip	英文	2016/02/01
74	38971	RuleID15448	採購單、付款、收據	.zip、.gz	英文	2016/08/08
72	41513	RuleID18688	訂購、付款、研討會	.zip	英文	2016/09/01
70	40056	RuleID6396	採購單、付款、收據	.rar	英文	2016/06/07
66	34796	RuleID5118	產品訂單、付款	.zip	德文、英文	2016/09/29
64	39317	RuleID4626 (cont)	發票、付款、出貨	.zip	英文、德文、西班牙文	2016/01/28
64	36917	RuleID4961KVR	確認、付款/轉帳、訂購、出貨	.zip	英文	2016/07/08
63	37179	RuleID13288	交貨通知、出庭、發票	.zip	英文、西班牙文	2016/07/21
61	38095	RuleID858KVR	出貨、報價、付款	.zip	英文	2016/08/01
58	39150	RuleID4961KVR	報價要求、採購單	.zip	英文、德文、多種語言	2016/01/25
47	41886	RuleID4961	轉帳、出貨、發票	.zip	英文、德文、西班牙文	2016/02/22

資料來源：思科資安研究部門

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

偵察 | 武器化 | 派送 | **安裝**

威脅一旦就位，就會在目標系統上安裝後門，讓惡意人士得以持續進入。

網路攻擊方法：「長尾」快照揭露使用者可輕易避免的威脅

所謂網路攻擊方法範圍的長尾（圖 20）包括收集用於攻擊鏈後期階段（「安裝」）的少量惡意軟體類型。在此階段中，銀行木馬、病毒、下載程式或某些其他攻擊套件等已傳送的威脅，會在目標系統中安裝後門，讓惡意人士可持續存取並有機會竊取資料、發動勒索軟體攻擊和進行其他傷害。

圖 20 所列出的威脅是除了前 50 種最常偵測到的惡意軟體類型以外，所發現的惡意軟體特徵碼樣本。網路攻擊方法的長尾，基本上是成功發動攻擊後可在機器或系統上暗中運作的威脅快照。這些感染多數是在遇到惡意廣告軟體或暴露於精心設計的網路釣魚詐騙時而最初孳生的。使用者通常可輕易避免或快速修復。

分享

圖 20 偵測到數量較少的惡意軟體樣本

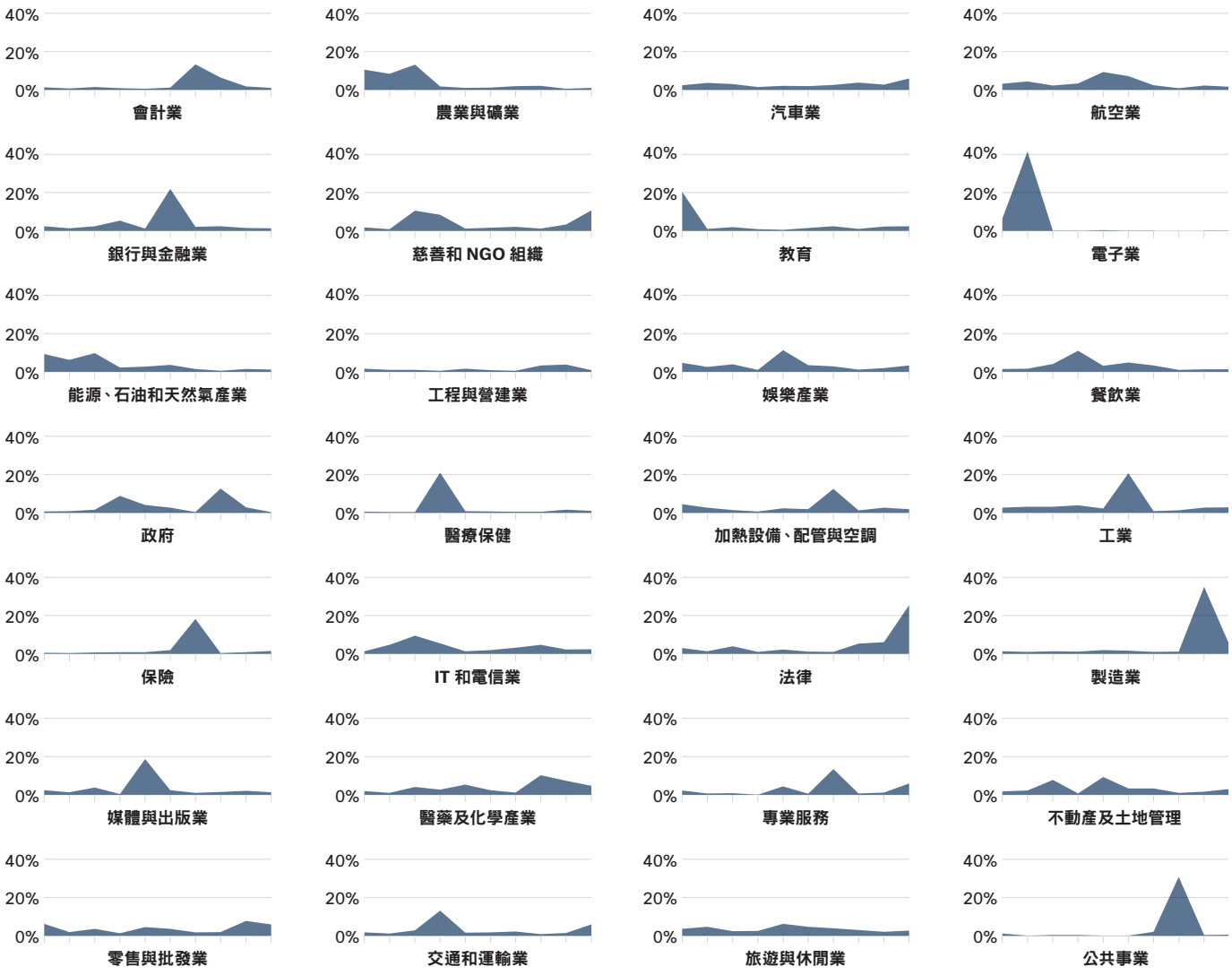
資料來源：思科資安研究部門

惡意軟體遇到的垂直風險：攻擊者會全面觀察價值

*思科 2016 年中網路安全報告*中有關惡意軟體風險的關鍵訊息是「所有垂直市場都不安全」。在我們的研究人員對每個產業的攻擊流量（「封鎖率」）以及「正常」或預期流量所做的定期檢視中，下半年已如實呈現此訊息。

我們注意垂直市場及其隨著時間推移的封鎖率（圖 21），在幾個月內的某些時候觀察到所有產業都曾經歷不同層度的攻擊流量。我們可以清楚發現隨著攻擊事件的增加和減少，其會在不同時間影響不同的垂直市場，無一倖免。

圖 21 每月垂直封鎖率百分比



資料來源：思科資安研究部門

分享

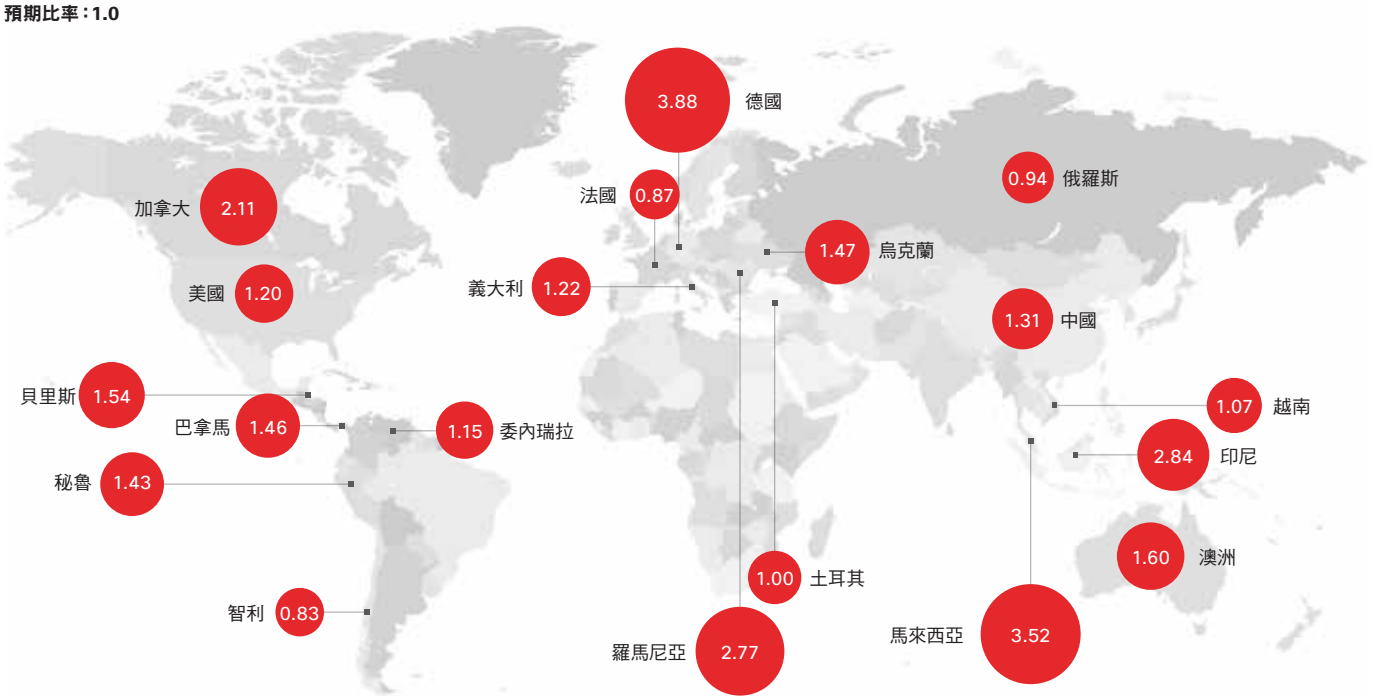
網路封鎖活動之區域概觀

惡意人士經常轉變活動基礎，並搜尋可發動活動的脆弱基礎架構。思科威脅研究人員可透過檢視整個網際網路流量及封鎖活動，提供有關惡意軟體來源的見解。

如圖 22 所示，來自美國的流量略增於*思科 2016 年中網路安全報告*中觀察到的封鎖率。美國擁有更大的封鎖市場佔有率，但這應該考慮到國家的線上流量市場佔有率在此發揮的作用。此外，美國是全球最大的惡意軟體攻擊目標。

提供給資安專業人員的重點是：區域網路封鎖活動與垂直網路封鎖活動類似，也顯示惡意軟體流量是全球問題。

圖 22 各國的網路封鎖率



資料來源：思科資安研究部門

分享

偵測用時：衡量防禦者進度的關鍵指標

思科持續改進衡量 TTD 的方法，以確保我們正在追蹤和報告最精確的 TTD 中位數評估。最近對我們的方法所進行的調整已針對第一次觀察到時分類為「不明」，並在持續分析和全球觀察後識別為「已知不良」的檔案，提升對其的能見度。我們透過更全面性的資料檢視，更可精確定位威脅第一次出現時，資安團隊確切需要多少時間才能判斷其是否為威脅。

此新見解已協助我們判斷 2015 年 11 月的 TTD 中位數為 39 小時。（請參閱**圖 23**）。到了 2016 年 1 月，我們已將 TTD 中位數降低至 6.9 小時。收集和分析 2016 年 10 月的資料後，我們的威脅研究人員判斷思科產品已在 2015 年 11 月到 2016 年 10 月這段期間，達到 14 小時的 TTD 中位數（請注意：2016 年的 TTD 中位數是觀察期間中位數的平均值）。

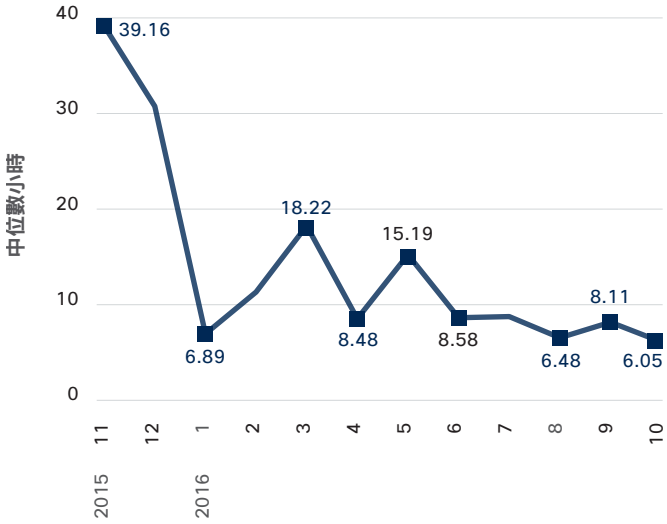
TTD 中位數在 2016 年有所波動，但整體呈下降趨勢。TTD 中位數提升表示惡意人士發動一波新威脅的時間。後續下降則反映防禦者佔上風，且可快速識別已知威脅的期間。

圖 23 也顯示 2016 年 4 月底的 TTD 中位數約為 15 小時，大於我們在*思科 2016 年中網路安全報告*中報告的 13 小時。[14] 該 15 小時是以從 2015 年 11 月到 2016 年 4 月收集的資料為基礎，而非使用修改的方法分析更詳細的追溯性檔案資訊來取得該數字。我們可以使用新的年中 TTD 數字，報告 2016 年 5 月到 10 月的 TTD 降低至約 9 小時。

檢閱追溯性資料不僅對判斷更精確的 TTD 中位數衡量，還對研究威脅如何隨著時間演進，都顯得相當重要。即使是威脅領域中的許多威脅對安全性社群而言眾所周知，但其仍特別無法捉摸，且可能需要較長的時間才能識別。

惡意人士會演進某些惡意軟體系列，以規避偵測並增加操作時間。此策略會阻礙防禦者取得和維護可偵測到許多已知威脅類型之優勢的進度。（如需更多此主題的相關資訊，請參閱第 34 頁的「演進時機：對某些威脅而言，改變持續不斷」）。但是，網路罪犯經常且快速演化威脅的事實顯示，他們面臨強烈且持續的壓力，為的就是要尋找可讓威脅持續活動和獲利的方法。

圖 23 TTD 中位數（月）



資料來源：思科資安研究部門

思科將「偵測用時」(TTD) 定義為：入侵發生以及偵測到威脅之間經過的時間。我們用來決定這段時間範圍所使用可選擇安全性遙測資料，是蒐集自思科部署在全球的資安產品。使用我們的全域能見度與持續分析模型，在遭遇所有未分類的惡意代碼時，我們將能測量惡意代碼開始在終端上執行，以及判定該代碼為威脅之間經過的時間。

[14] *思科 2016 年中網路安全報告*：**http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html**。

演進時機：對某些威脅而言，改變持續不斷

網路罪犯會使用各種混淆技術，讓惡意軟體保持強勁且可持續獲利。他們運用的兩種常見方法是演化承載傳送類型，以及迅速產生新檔案（擊敗僅雜湊適用的偵測方法）。我們的研究人員仔細檢視惡意人士如何使用這兩種策略，協助 Locky、Cerber、Nemucod、Adwind RAT、Kryptik 和 Dridex 等六種知名的惡意軟體系列規避偵測，並持續危害使用者和系統。

我們想要透過分析測量「演進時機」(TTE)：惡意人士需要改變特定惡意軟體傳送方式的時間，以及每次策略改變的時間長度。我們已分析來自不同思科來源的網路攻擊資料，特別是網路 Proxy 資料、雲端和端點進階惡意軟體產品，以及複合式防毒軟體引擎。

我們的研究人員期待變更由使用者系統定義且可傳送惡意軟體和檔案內容（或 MIME）類型的檔案副檔名。我們判斷出每種惡意軟體系列都具有獨特的演進模式。我們已針對每個系列檢視網路和電子郵件傳送方法的模式。我們也已追蹤與每種惡意軟體系列相關的唯一雜湊留存期，以判斷惡意人士如何快速建立新檔案（且因此具有新的雜湊）。

我們透過研究瞭解到：

- 勒索軟體系列的新二進位檔案似乎具有類似的循環。但是，Locky 會使用更多檔案副檔名和 MIME 組合傳送其承載。
- 某些惡意軟體系列只會運用一些檔案傳送方法，其他系列則會使用 10 種（含）以上的方法。惡意人士傾向長期使用有效的二進位檔案。在其他情況下，檔案快速出現和減少表示惡意軟體作者正在承受切換策略的壓力。
- Adwind RAT 和 Kryptik 惡意軟體系列具有較高的 TTD 中位數（如需有關 TTD 的更多資訊，請參閱第 33 頁）。我們也針對這些系列觀察到檔案留存期明顯混合的情況，這表示惡意人士重複使用已知難以偵測的有效二進位檔案。
- 我們注意 Dridex 惡意軟體系列的檔案留存期，影子經濟似乎可能已放棄使用這個曾經紅極一時的銀行木馬。Dridex 的偵測量在 2016 年底減少，用於傳送此惡意軟體的新二進位檔案開發情況也是如此。此趨勢表示惡意軟體作者不再認為演進此威脅具有任何價值，或已找到讓惡意軟體更難以偵測的全新封裝方式。

TTE 和 TTD

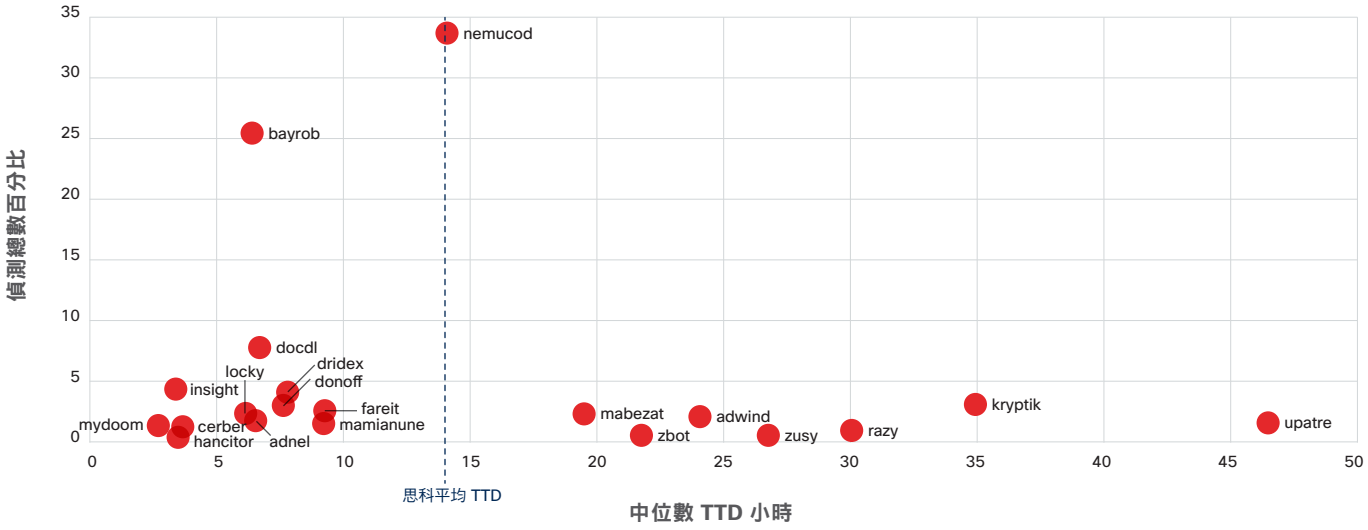
在我們在列於圖 24 的 TTE 研究中分析六種惡意軟體系列。該圖表描述我們的研究人員從 2015 年 11 月到 2016 年 11 月觀察到之前 20 名惡意軟體系列的 TTD 中位數（依偵測數排序）。我們在該期間的平均 TTD 中位數約為 14 小時（如需如何計算 TTD 的詳細資訊，請參閱第 33 頁）。

思科產品在 TTD 中位數時間內偵測到的許多惡意軟體系列是會快速傳播的工業化威脅，因此更為常見。Cerber 和 Locky 這兩種勒索軟體便是其中的範例。

惡意人士不需要費心演進（或完全不需演進）且年代久遠的常見威脅通常也會在 TTD 中位數時間內遭到偵測。範例包括 Bayrob（殭屍網路惡意軟體）、Mydoom（影響 Microsoft Windows 的電腦蠕蟲）和 Dridex（銀行木馬）等惡意軟體系列。

在下列幾節中，我們會呈現 Locky、Nemucod、Adwind RAT 和 Kryptik 惡意軟體系列 TTE 和 TTD 的研究重點。第 78 頁的附錄包括 Cerber 和 Dridex 的詳細發現。

圖 24 各頂尖惡意軟體系列 TTD 中間值（偵測數前 20 高的惡意軟體系列）



資料來源：思科資安研究部門

分享

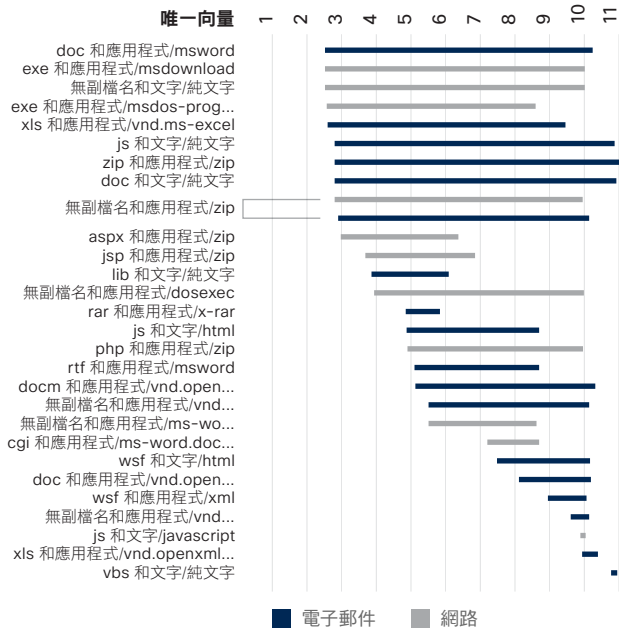
TTE 分析：Locky

我們透過 TTE 研究瞭解到 Locky 和 Cerber 採用數量有限的檔案副檔名和 MIME 組合，透過網路或電子郵件傳送惡意軟體。（請參閱圖 25）。我們已觀察包括與 Microsoft Word 相關之檔案內容類型的幾個組合（msdownload、ms-word）。但是，相關的檔案副檔名（.exe 和 .cgi）不會指回 Word 檔案。我們也已識別指向惡意 .zip 檔案的內容類型。

Locky 和 Cerber 似乎也經常使用新的二進位檔案以嘗試規避檔案偵測。Locky 惡意軟體系列的檔案留存期如圖 26 所示。圖表的上半部描述特定月份期間觀察到的檔案留存期。圖表的下半部顯示 Locky 相關雜湊量（同時包括新雜湊和先前觀察到的雜湊）的每月變化。

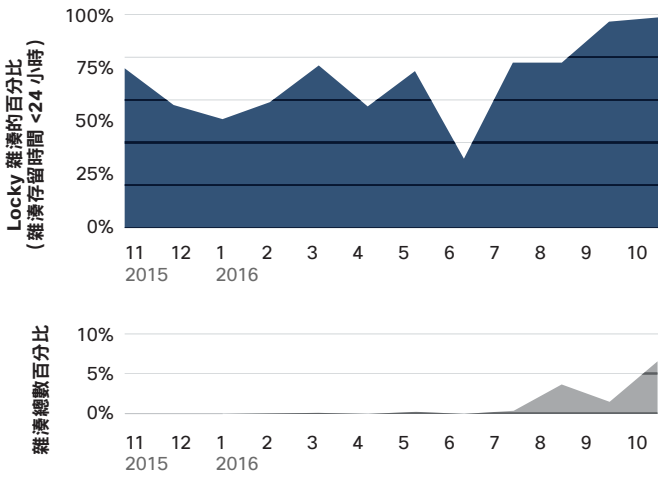
在圖 26 中，另請注意 6 月的雜湊量和檔案留存期分佈有所減少。以傳送 Locky 聞名的 Necurs 殭屍網路已在 6 月遭到殲滅，這可能讓惡意軟體的作者無法在該月份將惡意軟體保持最新狀態。但是，該惡意軟體很明顯快速地故態復萌。到了 7 月，惡意軟體已回復更標準的檔案留存期混合情況，且第一次偵測到時，大多數 (74%) 的檔案留存期都不到一天。

圖 25 造成及挾帶 Locky 酬載之威脅系列和標記的檔案副檔名/MIME 組合（網路和電子郵件向量）



資料來源：思科資安研究部門

圖 26 Locky 惡意軟體系列的雜湊壽命，以及各月觀察到的雜湊總數比例



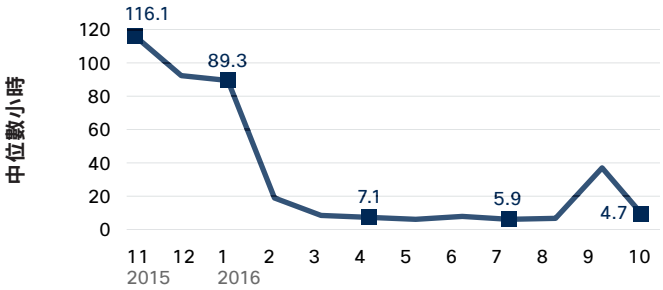
資料來源：思科資安研究部門

分享

我們對於此勒索軟體的二進位檔案快速循環並不感到驚訝。使用者通常會在 Locky 和 Cerber 執行個體推出的同一天或 1 到 2 天後偵測到該執行個體，這讓想要讓這些威脅保持活躍且有效的惡意人士必須持續演進這些威脅（如前所述，圖 24 顯示思科產品已在 2016 年的 TTD 中位數時間內偵測到 Locky 和 Cerber 勒索軟體）。

圖 27 顯示 Locky 勒索軟體的 TTD 中位數從 2015 年 11 月約 116 小時大幅降低至 2016 年 10 月的 5 小時。

圖 27 Locky 惡意軟體系列 TTD



資料來源：思科資安研究部門

TTE 分析：Nemucod

如圖 24 所示，Nemucod 在 2016 年是前 20 名惡意軟體系列中最常偵測到的惡意軟體。惡意人士會使用下載程式惡意軟體散佈勒索軟體及其他威脅，例如可促進點擊詐騙的後門木馬。Nemucod 的某些變種也可作為傳送 Nemucod 惡意軟體裝載的引擎。

圖 28 Nemucod 的檔案副檔名/MIME 組合（網路和電子郵件向量）

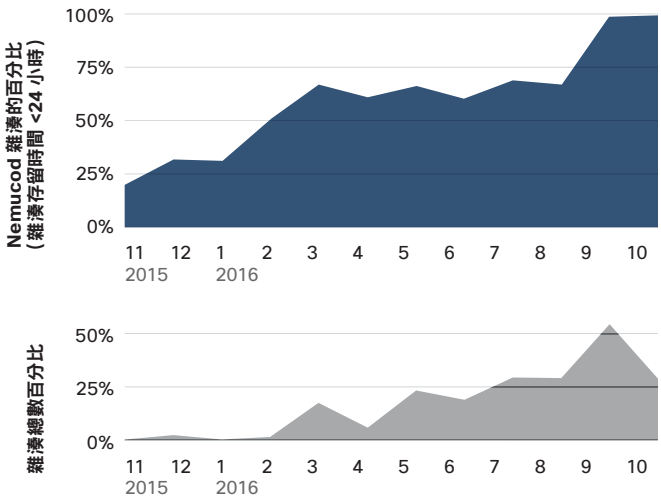
資料來源：思科資安研究部門

我們的威脅研究人員表示，Nemucod 惡意軟體在 2016 年如此常見的其中一個原因是其作者經常演進此威脅。思科已識別超過 15 個與 Nemucod 系列相關，且用於透過網路傳送惡意軟體的檔案副檔名和 MIME 組合。惡意人士會使用更多組合，透過電子郵件將威脅傳送給使用者（圖 28）。

許多檔案副檔名和 MIME 組合（網路和電子郵件）都是專為將使用者指向惡意 .zip 檔案或封存而設計。在我們觀察的月份期間，惡意人士也會重新使用許多組合。

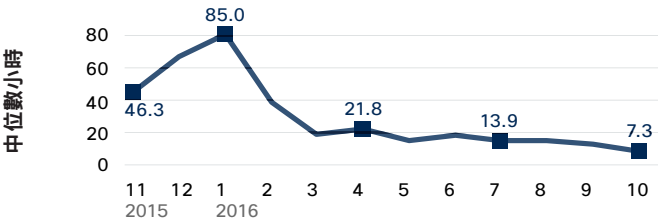
如圖 29 所示，許多偵測到的 Nemucod 雜湊留存期都不到 2 天。2016 年 9 月和 10 日，幾乎所有與 Nemucod 系列相關且已封鎖的二進位檔案留存期都不到一天。

圖 29 Nemucod 惡意軟體系列的雜湊壽命，以及各月觀察到的雜湊總數比例



資料來源：思科資安研究部門

圖 30 Nemucod 惡意軟體系列 TTD



資料來源：思科資安全研究部門

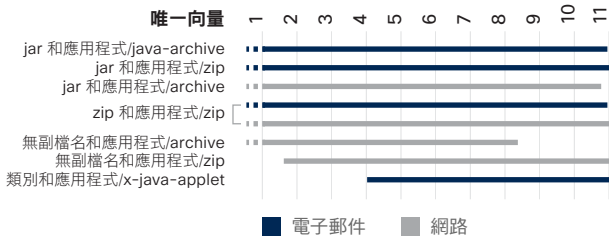
TTE 分析：Adwind RAT

思科威脅研究人員發現 Adwind RAT（遠端存取木馬）惡意軟體透過包括 .zip 或 .jar 檔案的檔案副檔名和 MIME 組合進行傳送，無論是透過電子郵件或網路攻擊媒介傳送惡意軟體都是如此。（請參閱圖 31）。

除了 9 月和 10 月觀察到的大多數檔案留存期都是 1 到 2 天以外，Adwind RAT 已在 2016 年大多數的觀察期間使用各種雜湊留存期（圖 32）。

我們也發現 Adwind RAT 的 TTD 中位數持續高於我們分析之其他惡意軟體系列的 TTD 中位數（圖 33）。惡意軟體的作者顯然已開發難以偵測的傳送機制，讓 Adwind RAT 得以獲致成功。因此，該惡意軟體不需要和在其他惡意軟體系列背後的操控者一樣經常或快速循環新雜湊。Adwind 木馬也可稱為 JSocket 和 AlienSpy 等。

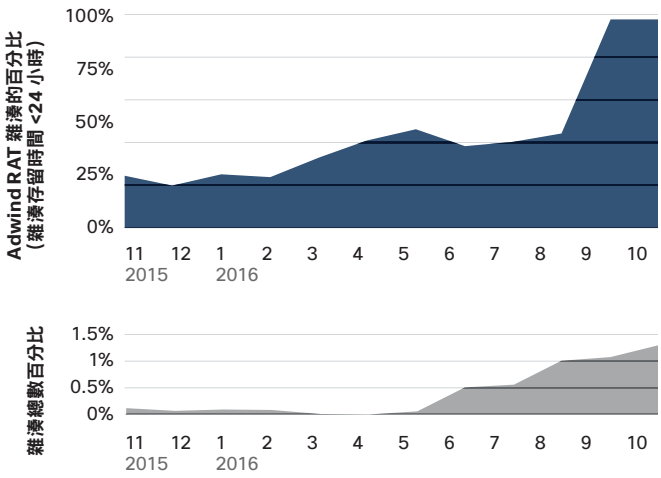
圖 31 Adwind RAT 的檔案副檔名/MIME 組合（網路和電子郵件向量）



資料來源：思科資安研究部門

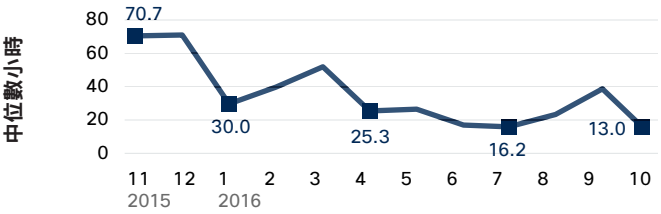
下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

圖 32 Adwind RAT 惡意軟體系列的雜湊壽命，以及各月觀察到的雜湊總數比例



資料來源：思科資安研究部門

圖 33 Adwind RAT 惡意軟體系列 TTD



資料來源：思科資安研究部門

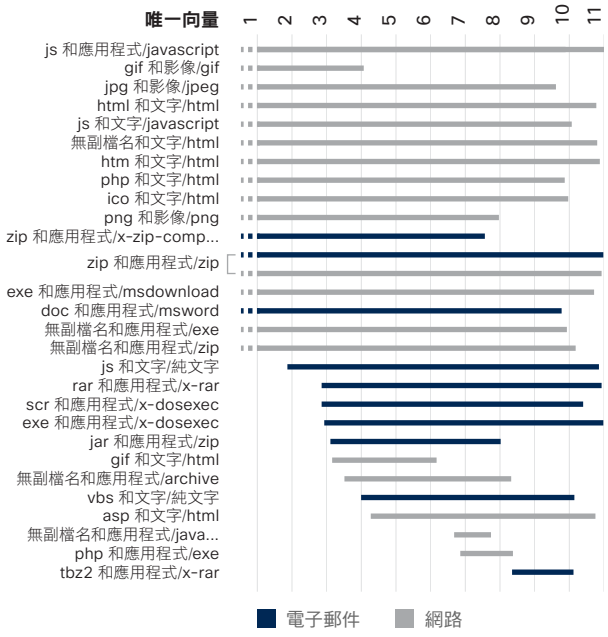
TTE 分析：Kryptik

在思科從 2015 年 11 月到 2016 年 10 月針對 TTE 所進行的研究中，Kryptik 與 Adwind RAT 惡意軟體一樣，具有持續高於其他惡意軟體系列的 TTD 中位數（約 20 小時）（圖 36）。但是，到了 10 月，思科產品對 Kryptik 惡意軟體的 TTD 窗口已降低至不到 9 小時（圖 36）。

特別是在 2016 年上半年，相較於我們分析的其他惡意軟體系列，Kryptik 惡意軟體系列也已使用更多的雜湊留存期。Kryptik 作者的能力長期依賴留存期較長的雜湊，表示防禦者已難以偵測到此惡意軟體類型。

在我們的觀察期間，Kryptik 的作者已透過網路攻擊媒介採用各種裝載傳送方法。作者已針對網路和電子郵件，在檔案副檔名和 MIME 組合中使用 JavaScript 檔案和封存檔案（例如 .zip 檔案）（請參閱圖 34）。某些組合可追溯到 2011 年。

圖 34 Kryptik 的檔案副檔名/MIME 組合（網路和電子郵件向量）

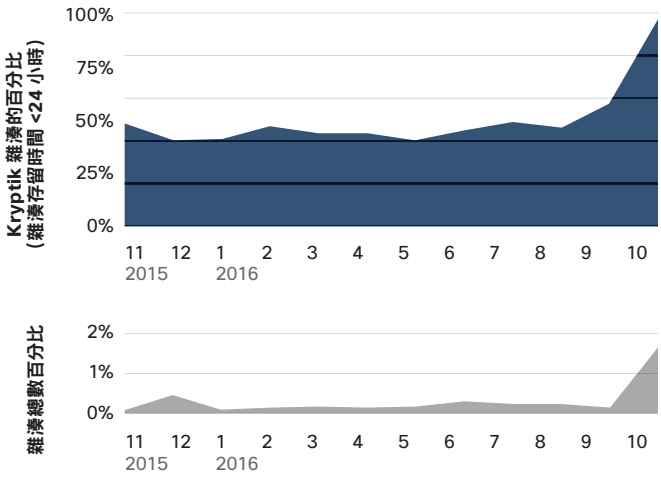


資料來源：思科資安研究部門

分析這 6 種惡意軟體系列後，我們發現惡意人士必須經常變換策略，以利用緊迫的有限時間內順利操作威脅。這些調整則顯示出即使威脅經過演進，防禦者仍可迅速偵測到已知的惡意軟體。攻擊者承受壓力，為的就是要找出規避偵測且能讓威脅活動獲利的新方法。

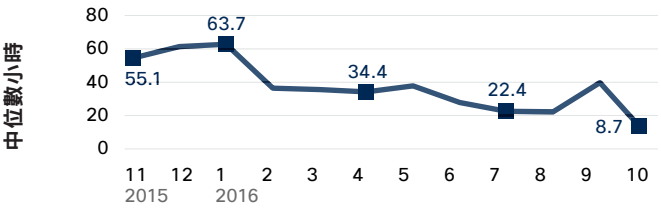
在這快速演進且所有惡意軟體系列都具有不同行為的複雜領域中，人類專家和單點解決方案不足以快速識別和因應威脅。可針對威脅提供即時深入分析並自動偵測和防禦的整合式安全性架構，是改善 TTD 及確保在發生感染時能快速修復的基礎。

圖 35 Kryptik 惡意軟體系列的雜湊壽命，以及各月觀察到的雜湊總數比例



資料來源：思科資安研究部門

圖 36 Kryptik 惡意軟體系列 TTD



資料來源：思科資安研究部門

防禦者行為

防禦者行為

2016 年漏洞數量下降

根據我們的研究顯示，在 2016 下半年廠商揭露的弱點數量從 2015 年開始大幅下降（圖 37）。美國國家安全漏洞資料庫也顯示類似的下降趨勢。顧問也不太清楚為何揭露漏洞的數量會下降。

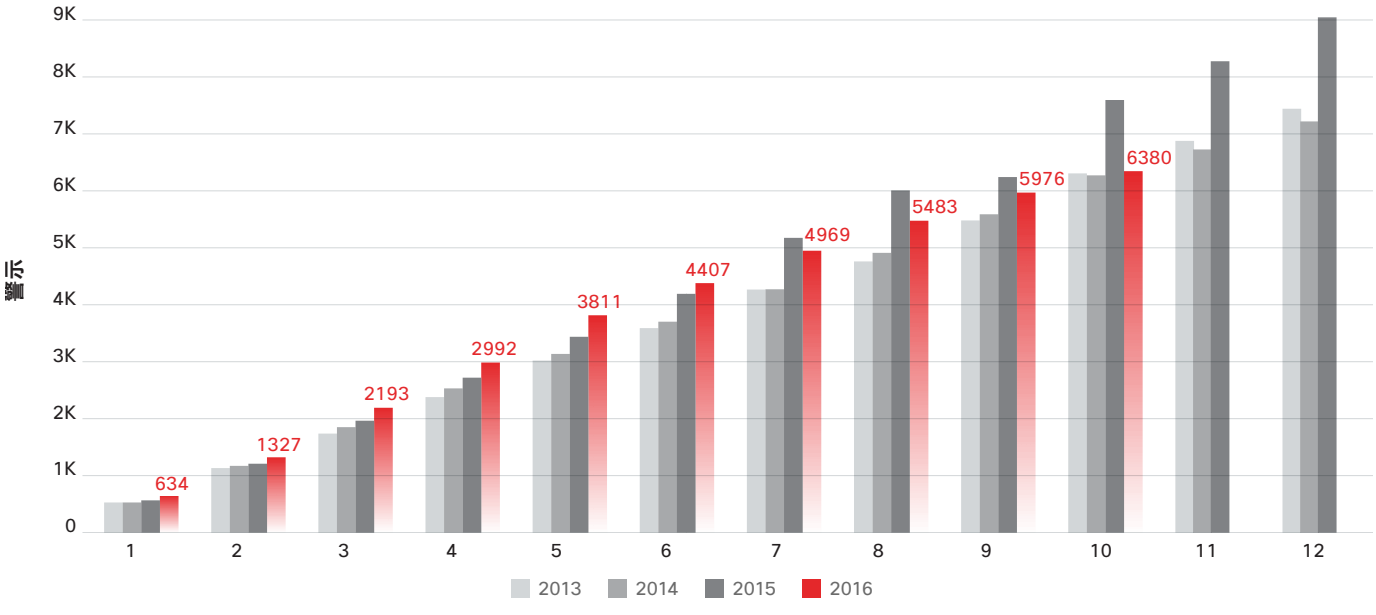
不過值得注意的是，2015 年是漏洞異常活躍的一年，因此 2016 年的數字可能反映出漏洞顧問的正常步調。2015 年 1 月到 10 月的警示總數達到 7602 則。2016 年同期警示總數達到 6380 則；2014 年同期警示總數為 6272 則。

2015 年出現大量的弱點報告，這可能表示廠商更密切觀察現有的產品和程式碼、更謹慎地執行安全開發生命週期 (SDL) 實務，以及識別弱點並後續進行修正。回報弱點的數量下降，可能表示這些努力已有所回報。換句話說，在產品上市之前，廠商現在會專注於識別弱點並予以修正。

在 2016 年，Apple 是弱點數量下降幅度最大的廠商：該公司在 2015 年回報 705 個弱點，而在 2016 年回報 324 個弱點（下降 54%）。思科也在 2015 年回報 488 個弱點，並在 2016 年回報 310 個弱點（下降 36%）。

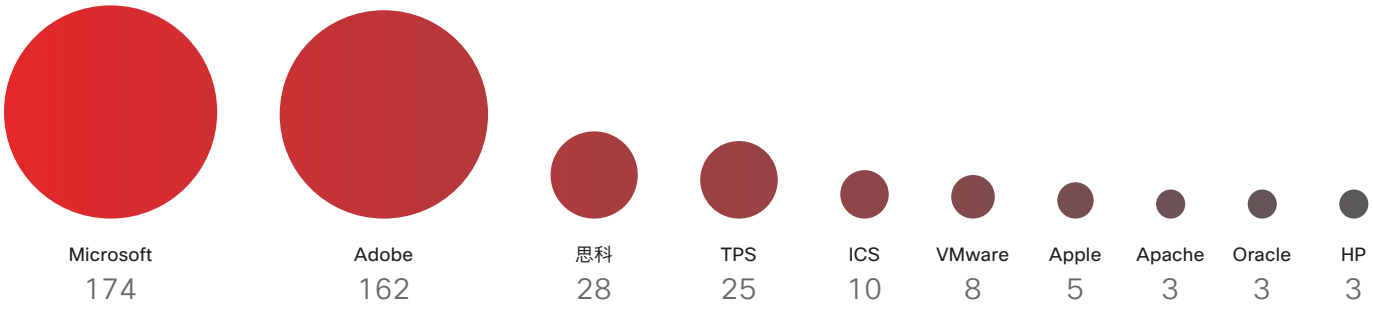
在安全研究人員之間產生的疑慮是，這會導致資安專業人員發生「弱點疲勞感」的情況。最近幾個月都未發佈讓整個產業引起軒然大波的重大弱點公告，就像 2014 年 Heartbleed 事件一樣。事實上，大肆宣傳 Heartbleed 等「冠名」的弱點和 2015 年弱點數量增加的消息，可能會導致某種程度的疲勞感，或至少會對回報弱點較不感興趣。

圖 37 年度累積警示總計



資料來源：思科資安研究部門

圖 38 依廠商和類型排列的重大弱點顧問



資料來源：美國國家安全弱點資料庫 (NVD)

思科目前使用嚴重性/影響評分 (SIRs)，評分等級包括「重大」、「高度」、「中度」和「低度」，其可對應至常見弱點評分系統 (CVSS) 的簡化版評分優先順序。此外，思科已經採用 CVSS v2.0 之後的 CVSS v3.0，此變更可能使得部分弱點的評分高於以往，所以資安專業人員會發現評為「重大」和「高度」的弱點稍微增加，而非「中度」和「低度」。如需評分變動的詳細資訊，請參閱 Cisco Security 部落格文章：資安弱點評分的演進：續集。

在思科 2017 年資安能力基準研究（第 49 頁）中，資安專業人員表示他們對資安操作的認同感有稍微降低的情形，而此種現象可能與需要持續升級和修補的「疲勞感」相關。例如，2016 年有 53% 的資安專業人員表示非常同意定期、正式且有策略地審查並改善資安實務；而 2014 年和 2015 年則有 56% 表示非常同意。

當然，弱點數量下降應不至於對威脅情勢產生過度的自信：即使未出現高能見度的弱點，所有人都不應該對威脅掉以輕心。

如同我們在先前報告中的建議，資安專業人員應該齊心協力列出修補程式的優先順序。如果缺乏人力及其他資源，而無法及時安裝所有可用的修補程式，請評估最能維護網路安全的修補程式，並將其列在待辦事項清單的最上層。

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

圖 39 精選重大弱點顧問

顧問標題	發行日期
Adobe Acrobat 和 Acrobat Reader 記憶體毀損程式碼執行弱點	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損遠端程式碼執行弱點	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 7 月 21 日
Adobe Acrobat 和 Acrobat Reader 整數溢位弱點	2016 年 5 月 23 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損遠端程式碼執行弱點	2016 年 2 月 8 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 7 月 23 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 5 月 24 日
Adobe Acrobat 和 Acrobat Reader 記憶體毀損弱點	2016 年 5 月 23 日

資料來源：思科資安研究部門

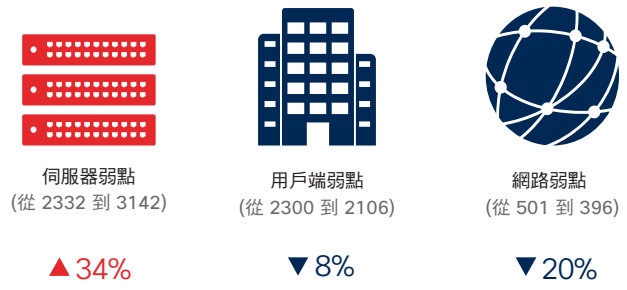
以上所列的是 2016 年評分為重大的精選弱點顧問。根據多項來源的報告，這些弱點不是具有可公開取得的攻擊程式碼，就是遭到肆無忌憚地攻擊。

伺服器和用戶端弱點

如*思科 2016 年中網路安全報告*所述，惡意人士正在尋找可在伺服器端解決方案中活動的空間和時間。在伺服器軟體內發動攻擊，他們才可能控制更多的網路資源，或在其他重要的解決方案之間橫向移動。

思科研究人員已依照各廠商來追蹤主從式弱點（圖 40）。

圖 40 主從式弱點分析，2015—2016



資料來源：美國國家安全弱點資料庫

中介軟體：惡意人士在未修補軟體上看到了契機

我們已在*思科 2016 年中網路安全報告*中分享攻擊伺服器端系統的相關資料。連接平台或應用程式的中介軟體準備在 2017 年吸引尋求可操作空間的攻擊者，而這些地方連防禦者也無法及時回應或辨識威脅。

思科研究人員在尋找第三方軟體中的弱點時，每個月平均發現 14 個新的軟體弱點。這些弱點（62 個）大多數是因為使用中介軟體。在這 62 個弱點當中，有 20 個是在處理 PDF 的程式碼中發現；有 12 個在處理影像的程式碼中發現；有 10 個在一般辦公室生產力解決方案的程式碼中發現；9 個在壓縮程式碼中；有 11 個則在其他程式庫中發現（圖 41）。

中介軟體的弱點會造成獨特的資安威脅，因為中介軟體的程式庫通常不會像用戶端面臨的軟體一樣迅速更新，也就是說這種軟體每天都會直接與使用者互動，例如生產力解決方案。中介軟體程式庫可能不會經過軟體稽核，因此弱點仍會保留在原處。

圖 41 在中介軟體程式庫中發現的弱點

資料來源：思科資安研究部門

分享

組織可能要孤注一擲猜哪一個中介軟體是安全的，也可能要更加注意高能見度解決方案的更新。不過，他們可能下錯注，惡意人士不會透過這些低調的途徑入侵網路。中介軟體便成為了防禦者在安全性的盲點，也向攻擊者提供了契機。

由於許多中介軟體解決方案來自開放原始碼開發人員，更新中介軟體程式庫的挑戰便與開放原始碼軟體的問題密切相關（如*思科 2015 年中網路安全報告*所述）。（但是，眼前的問題會同時影響開放原始碼和專屬中介軟體開發人員）。如此一來，中介軟體程式庫可能會依賴多位開發人員，以保持在最新狀態。在負擔過重的 IT 或資安團隊所需要管理的工作清單中，中介軟體程式庫更新可能不是首要之務，但應該要投入更多心力。

惡意人士入侵中介軟體弱點，將會帶來何種潛在的影響呢？考量到中介軟體及其他重要系統之間的連接媒介，例如電子郵件或訊息，攻擊者可橫向進入這些系統並傳送網路釣魚訊息或垃圾郵件。或者，攻擊者也可以偽裝為已授權的使用者，濫用與使用者之間的信任關係，以取得進一步的存取權。

若要避免淪為透過中介軟體弱點而發動攻擊的受害者，您應該要：

- 在您使用的應用程式中，主動維護已知相依性和程式庫的清單
- 主動監控這些應用程式的安全性，並盡可能減輕風險
- 在與軟體廠商的合約中附上服務等級協定，以及時提供修補程式
- 經常稽核和審查軟體相依性和程式庫的使用情況
- 要求軟體廠商提供如何維護和測試其產品的詳細資訊

總而言之，延遲進行修補會提升攻擊者可操作的空間，並讓他們有更多時間可以控制重要系統。在下一節中，我們將探討修補一般生產力解決方案（例如網頁瀏覽器）的影響和趨勢。

修補時間：縮短補救期

許多使用者不會及時下載並安裝修補程式，讓惡意人士可以利用這些尚未修補的漏洞侵入網路。我們在最新的研究中發現，若要鼓勵使用者下載並安裝修補程式，關鍵在於廠商提供軟體更新的步調。

對攻擊者而言，安全性修補程式的發佈其實是在暗示有可趁之機。即便可能早有攻擊者曾經利用漏洞，但是修補程式的通知等同於在向其他攻擊者表明舊版門戶洞開。

如果軟體廠商依照規律的排程發佈新版本，使用者就會習慣下載及安裝更新版本。相反地，如果廠商升級版本的時間不固定，使用者比較不可能進行安裝，而繼續執行過時而具有入侵漏洞的解決方案。

其他會影響升級週期的行為包括：

- 提醒訊息的干擾程度
- 選擇取消的容易程度
- 軟體的使用頻率

廠商發佈升級版本後，使用者進行安裝的間隔會因人而異。我們的研究人員調查了客戶在端點上安裝軟體的情形，並把安裝的軟體分為三類：

- **新版**：端點執行軟體的最新可用版本
- **近期版本**：端點執行最近三個版本之一的軟體，但不是最新版本
- **舊版**：端點執行最近三個版本以前的軟體

舉例來說，如果廠商在 2017 年 1 月 1日發佈第 28 版，代表第 28 版為新版，第 26 版為近期版本，第 23 版則屬舊版。（下一頁的圖例為一或多個軟體版本的發行週數。）

分析 Adobe Flash（圖 42）的使用者時，我們發現在更新版本發佈的第一週內，有近 80% 的使用者安裝最新的軟體版本。換句話說，軟體只用了一週左右的時間，使用者就已跟上最新版本。我們將這一週稱為「補救期」，而駭客入侵正是利用這個時期入侵。

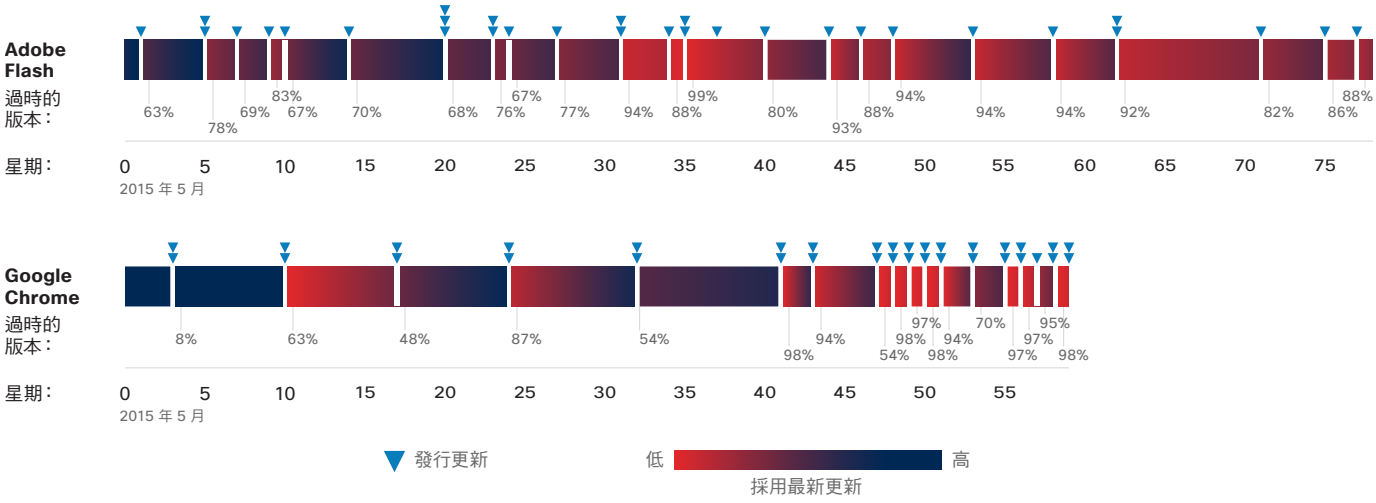
在 Adobe Flash 圖表的 2015 年第四季後期中，可以看到現該解決方案的最新版本使用者數量銳減。我們在檢視該時期時，發現 Adobe 竟在短時間內連續發佈五種 Flash 版本，內容包含多種新增功能、錯誤修復及安全性更新。如此「慌忙」的更新可能會讓使用者混淆，進而質疑是否需要下載這麼多的更新，對升級通知的數量感到厭煩，或者覺得自己已經下載過重大更新，而而忽略新的通知。無論他們不願下載更新的原因為何，這對提供防禦的廠商而言都不是好事。

Google Chrome 網頁瀏覽器則有不同的升級模式，他們的升級步調相當規律，也訂有嚴格的取消政策，使用者很難忽略更新通知。如圖 42 所示，執行最新版本的端點在數週期間內相對穩定。

根據資料顯示，Chrome 補救使用者的時間相對較短，規律更新的補救時程約為一週。然而，2016 年第二季至第三季的 9 週期間卻出現了七次更新。這段期間雖有補救使用者，他們卻也對升級感到厭煩。即使補救了大部分的使用者，維持舊版的使用者比例卻見穩定成長。

Mozilla 的 Firefox 瀏覽器同樣也是固定更新，但是發佈更新後的補救期長達一個月。也就是說，Firefox 使用者下載並安裝的頻率不及 Chrome 的使用者，而其中一個原因可能是部分使用者不常使用該瀏覽器，所以沒有看到及下載更新（詳見次頁圖 43）。

圖 42 修補 Adobe Flash 和 Google Chrome 的時機



資料來源：思科資安研究部門

我們發現，Firefox 大約每隔一週更新版本一次，但這在我們的觀察期中有增加的情形。頻率的增加見於舊版 Firefox 使用者人數的成長，其補救期約為 1.5 週，但是時間經常重疊。維持最新版本的人數跌至所有使用者的 30%，甚至曾有高達三分之二的使用者，只想執行比最新版本舊四個版本以上的瀏覽器。因此，雖然 Firefox 能夠快速地解決問題及修復錯誤，使用者卻未依照相同的頻率更新及重新啟動。

對軟體而言，使用程度似乎也可做為漏洞的指引。如果使用者不常使用軟體，因而不知道需要修補和升級，這種被忽略的軟體便會讓攻擊者有入侵的空間與時間。

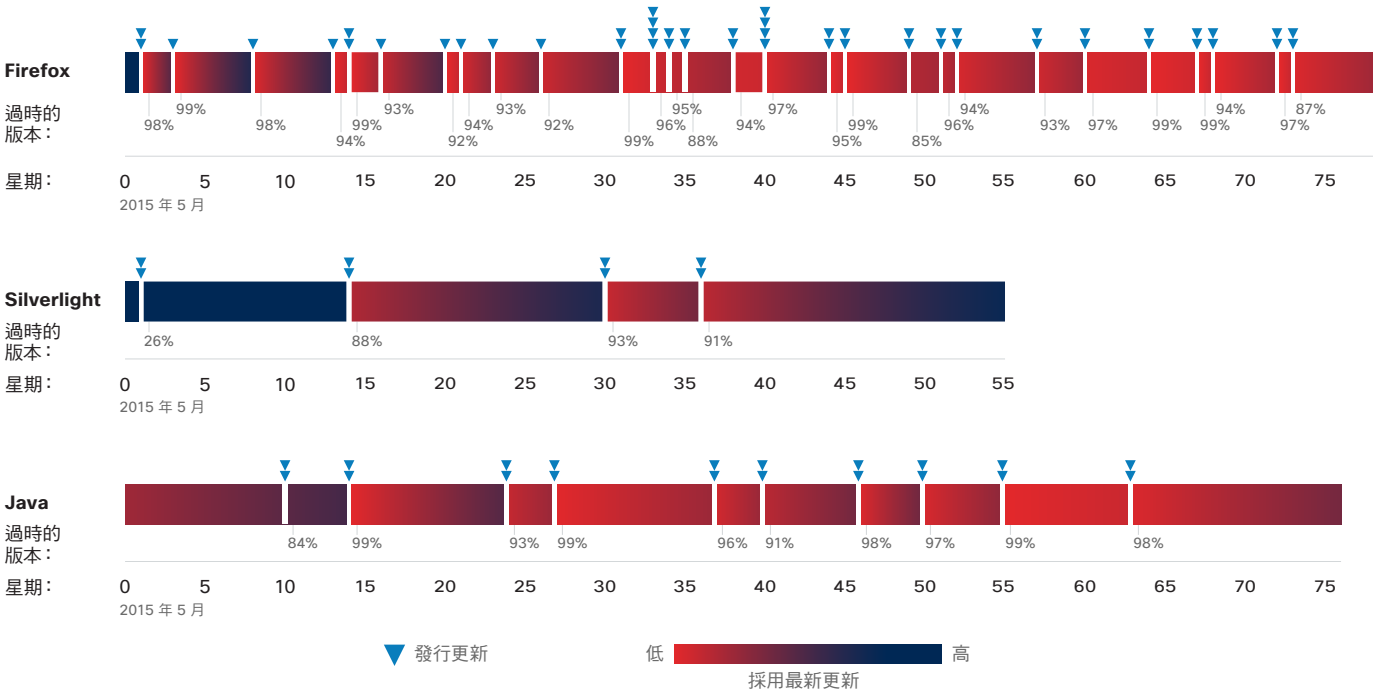
這點可從我們對 Microsoft Silverlight 的研究中看得出來，其在發佈後讓使用者安裝升級的補救期長達 2 個月。該軟體曾在 5 週內發佈更新兩次，對使用者的影響超過 3 個月，如 2015 第四季至 2016 年第一季所示。

Microsoft 雖於 2012 年宣佈終止 Silverlight，但至今仍會發佈修補程式與錯誤修復。然而，Silverlight 卻造成與 Internet Explorer 如出一轍的問題：過時且尚未修補的軟體容易遭到攻擊者入侵。

Java 使用者補救期的資料顯示，大多數的使用者都是執行最新軟體版本的前一至三個版本，補救期約為 3 週。Java 特別的地方就在於大部分的使用者都是使用近期版本，而其更新週期介於 1 至 2 個月之間。

綜上所述，從各種修補週期的案例中可以得知，升級的發佈模式對使用者安全性形勢而言是個重要的因素，不甚者可能會將網路致於險境。

圖 43 修補 Firefox、Silverlight 及 Java 的時機



資料來源：思科資安研究部門

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

思科 2017 年
資安能力基準研究

思科 2017 年資安能力基準研究

為了評估資安專業人員在組織中的情況，思科曾向數個國家/地區及各種規模組織的安全主管 (CSO) 及安全作業 (SecOps) 管理員，詢問他們對安全性資源和程序的想法。「2017 年思科資安能力基準研究」深入探討目前使用的資安作業及資安措施成熟度，並且以 2015 年和 2016 年的研究結果做為比較。本研究共有 2900 多位受訪者，分別來自 13 個不同的國家/地區。

資安專業人員無不希望所屬的組織更安全，但是要能因應捉摸不定的敵方情勢，應付攻擊者想要擴大戰場的野心。許多組織會同時仰賴於多家廠商提供的眾多解決方案，這卻會隨著網際網路的速度、連接裝置和流量持續增長，而增加保護網路的複雜與混淆程度。組織想要自我防護，就必須從簡及整合。

看法：資安專業人員對工具有信心，但較不確定是否能夠有效地利用

大多數的資安專業人員認為自己具有足夠的解決方案，且安全性基礎架構也是最新版本。然而，我們的研究顯示，他們的信心伴隨著某種不確定感。並非所有的專業人員都確定自己可以集合預算和人力，進而真正地善用自有的技術。

組織的威脅來自四面八方，惡意人士既機伶又創新，總是能比防禦機制聰明。即使身處草木皆兵的的環境，大部分的資安專業人員仍深具信心，認為自己的安全性基礎架構為最新版本（不過，他們的信心程度在近年來有稍微下降的趨勢）。在 2016 年，58% 的受訪者表示，他們使用的是最新版安全性基礎架構，並且經常使用最新的技術進行升級。37% 的受訪者則表示，他們會定期更換或升級安全防護技術，但是並未配備最新最好的工具（圖 44）。

圖 44 認為安全性基礎架構為最新狀態的資安專業人員百分比

資料來源：思科 2017 年資安能力基準研究

此外，三分之二以上的資安專業人員認為，他們的安全性工具非常有效或極度有效。例如，74% 的受訪者相信，他們的工具在已知資安威脅的封鎖方面非常或極度有效，而 71% 認為自己的工具能有效偵測網路異常，並能因應百變的威脅種類進行動態防禦（圖 45）。

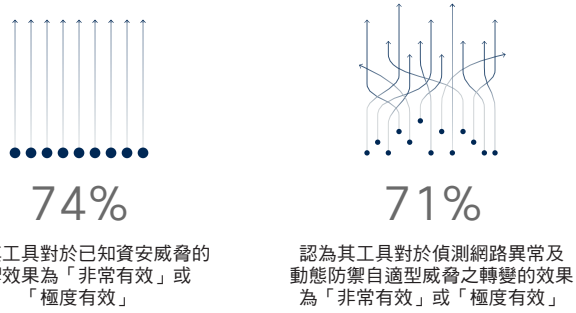
問題在於，對工具的信心不一定等於有效的安全防護。研究指出，資安部門時常為眾多廠商的複雜工具所苦，還要擔憂內部缺乏專業的人才，進而產生「理想面對現實」的難題。資安專業人員想要簡單又有效的安全性工具，卻沒有整合的作法可以實現這個理想。

資安仍是許多組織高層的優先要務，資安專業人員也相信，領導階層把資安列為組織的主要目標。因此，他們的挑戰自然是要符合領導階層的支持，找出可能影響安全防護結果的人才和技術。

在 2016 年，非常同意領導階層將資安視為優先要務的資安專業人員比例為 59%，而 2014 年和 2015 年分別為 63% 和 61%，呈現稍微下降的趨勢（圖 46）。2016 年有 55% 的資安專業人員同意，資安角色與職責在組織的執行團隊中有明確的劃分，而 2014 年和 2015 年同為 58%。

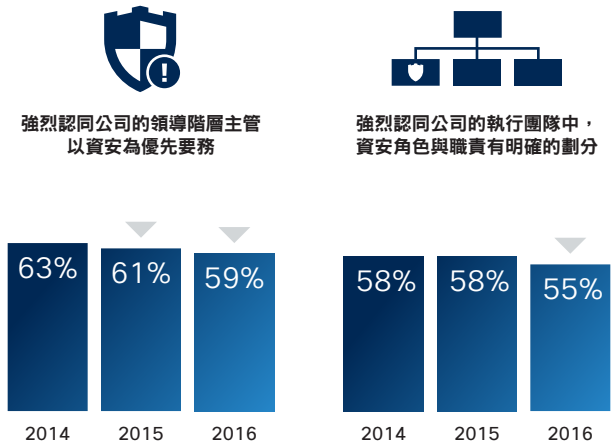
整體而言，資安專業人員對自己的工具深具信心，並且可以說服公司的領導階層解決資安問題。然而，這樣的自信卻有稍微降低的現象。資安專業人員攻擊者開始注意到攻擊者得逞，感受到面對攻擊規模不斷擴大的無能為力。

圖 45 發現各種強效安全性工具的資安專業人員百分比



資料來源：思科 2017 年資安能力基準研究

圖 46 認為資安是經營管理層級之優先要務的資安專業人員百分比，2014–2016



資料來源：思科 2017 年資安能力基準研究

限制：時間、人才和金錢都會影響威脅應變能力

如果資安專業人員較有信心，相信自己擁有可以偵測威脅及降低損壞的工具，他們同時也體悟到，某些結構性限制阻礙了他們達成目標。預算吃緊就是一個始終存在的難題，不過還有其他限制有效資安的因素，造成安全防護簡化及自動化的困難。

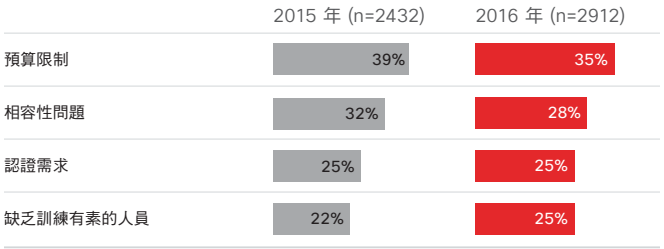
在 2016 年，35% 的資安專業人員表示，預算是他們在採用進階資安程序和技術時的最大阻礙（2015 年則有 39% 將其視為最大阻礙，比例稍微下降），如**圖 47** 所示。至於第二常見的阻礙，2015 年和 2016 年則都顯示為與舊版系統的相容性問題，比例分別為 32% 和 28%。

預算只是其中一個問題，其他像是相容性問題，就會造成系統各自為政而無法整合。另外還有卻乏受過訓練的人員，這樣的隱憂凸顯出一個問題：只有工具而沒有人才，因此無法真正地了解資安環境中的局勢。

若考量到因應針對性的攻擊和百變的攻擊戰術需要專業知識和決策能力，缺少人才確實是一個大問題。除了擁有正確的工具之外，IT 資安團隊也必須具備豐富的資源和專業，才能使技術和政策相互配合，進而達到更好的資安結果。

在受訪組織中，資安專業專業人員的中位數為 33，而 2015 年為 25。在 2016 年，19% 的組織有 50 至 99 位專責的資安專業人員，9% 有 100 至 199 位，12% 多達 200 位以上（**圖 48**）。

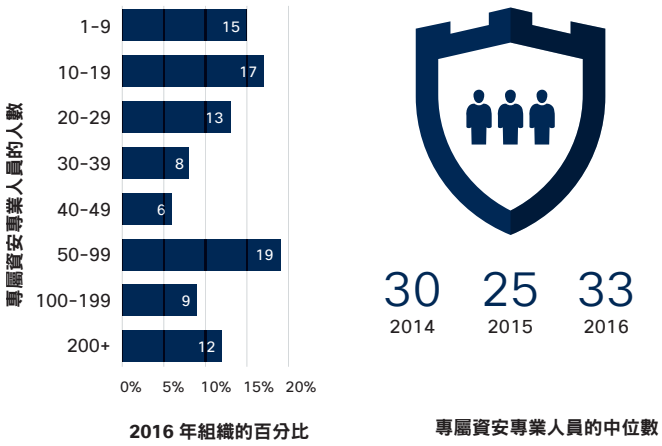
圖 47 阻礙資安的最大障礙



資料來源：思科 2017 年資安能力基準研究

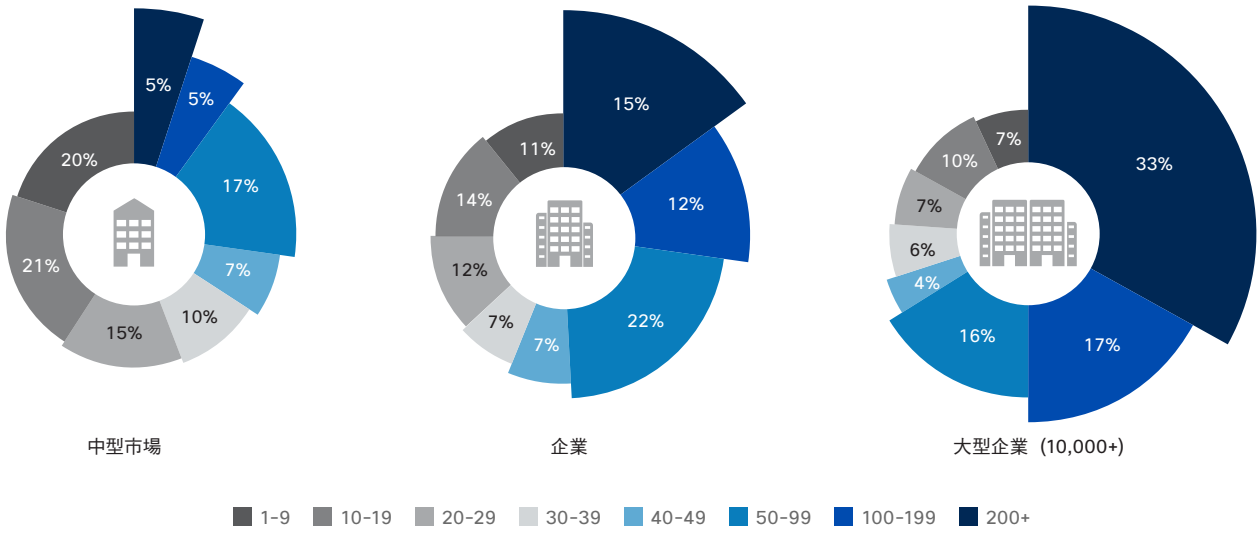
分享

圖 48 組織聘雇的資安專業人員數量



資料來源：思科 2017 年資安能力基準研究

圖 49 依據組織規模排列的資安專業人員數量



資料來源：思科 2017 年資安能力基準研究

分享

資安專業人員的人數會因組織規模而異。如圖 49 所示，33% 的大型企業（員工超過 10,000 人）有 200 位以上的資安人員。

無論限制因素為何，專業性人員都必須回答一些難解的問題，瞭解限制自身能力的障礙何在，才能面對未來的威脅。

例如，多少的預算才算真正足夠？根據調查受訪者的回答，資安團隊必須與公司的其他優先要務競爭，甚至在 IT 團隊中也是如此。如果拿不到預算來添購更多的工具，表示他們必須更加善用現有的資金。例如，透過自動化來彌補有限的人力。

類似的問題還包括軟硬體的相容性問題：隨著相容性問題的不斷增加，究竟需要管理多少版本的軟硬體（而且大多數可能還無法有效操作）？資安團隊該如何處理必要的多種認證要求？

委外和雲端有助於節省預算

許多參與基準研究的安資安專業人員認為他們採購資安商品的資金不足。他們藉由將某些工作委外或使用雲端解決方案來節省預算。他們也必須仰賴自動化。

除了上述限制之外，資安專業人員也不那麼重視資安操作化。此一趨勢使人產生疑慮：資安專業人員所建立的不是最為理想的安全性基礎架構。這種越來越不重視操作化的跡象，可能表示組織尚未準備好防禦攻擊範圍逐漸擴增的情勢。

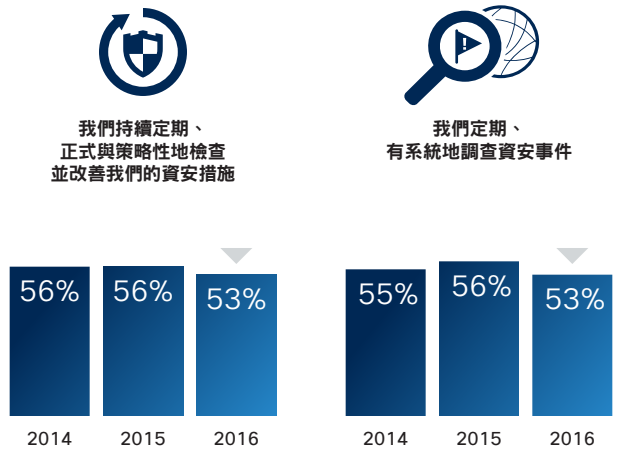
舉例來說，2016 年有 53% 的受訪者非常同意，他們有持續定期、正式且策略性地檢查並改善安全措施，2014 年和 2015 年則同為 56%。相較於 2014 年的 55% 和 2015 年的 56%，2016 年也有 53% 的受訪者表示非常同意定期且有系統地調查資安事件（圖 50）。

如果資安專業人員沒有達成應用資安的目標，想必他們也無法有效部署現有的工具，更遑論增加新工具了。根據研究受訪者的回答，他們無法使用手中現有的技術，而是需要易操作的簡化工具，以便將安全性程序自動化。這種工具必須提供全面的局勢分析，告知網路環境中的一舉一動。

無法整合資安可能會造成時間和空間的漏洞，致使惡意人士得以發動攻擊。資安專業人員對多家廠商提供的解決方案和平台舉棋不定，更可能會讓事情更加複雜，而難以建立天衣無縫的防禦機制。如圖 51 所示，大多數公司在環境中應用的資安廠商和資安產品都超過五種。55% 的資安專業人員至少使用六家廠商，45% 借助於一至五家廠商，65% 使用六種以上的產品。

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

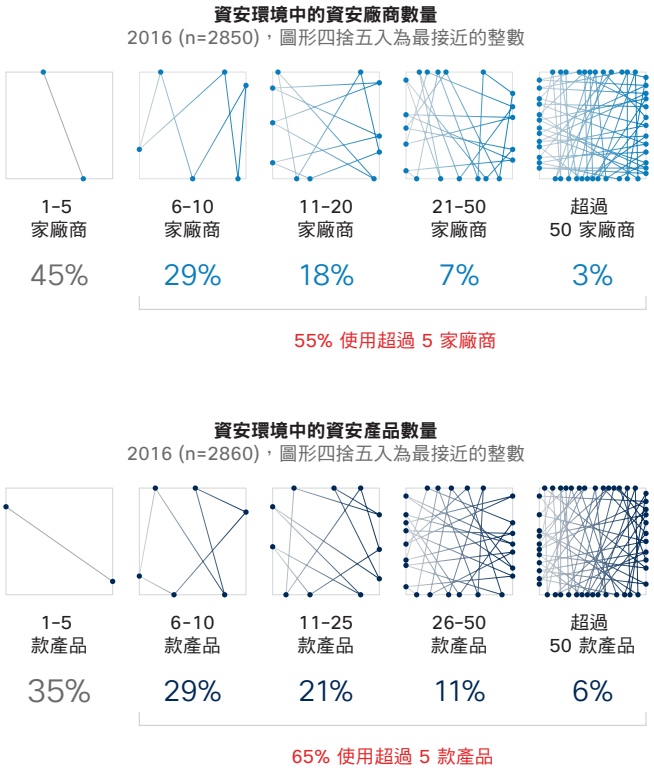
圖 50 非常同意安全性操作化聲明的受訪者百分比



2014 (n=1738), 2015 (n=2432), 2016 (n=2912)

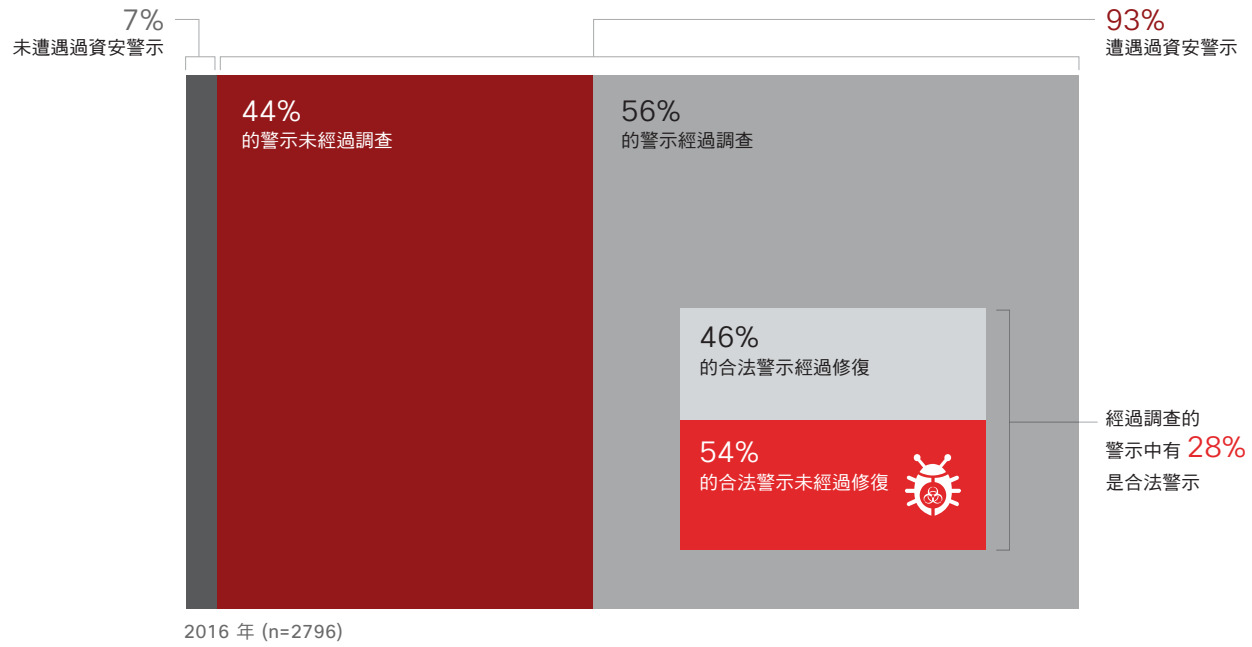
資料來源：思科 2017 年資安能力基準研究

圖 51 組織使用的資安廠商和產品數量



資料來源：思科 2017 年資安能力基準研究

圖 52 未調查或未修復之資安警示的百分比



資料來源：思科 2017 年資安能力基準研究

如果操作化目標失利、工具無法發揮最大效用，且人力又不夠健全，下場只會是搖搖欲墜的資安環境。資安專業人員會被迫取消警示的調查，只因為他們沒有人才、工具或自動化解決方案，而無法判定警示的重要程度和發生原因。

或許是許多因素（如缺少整合的防禦系統，或工作人員沒有時間）所致，在組織一天內收到的資安警示中，只有稍微超過一半的警示受過調查。如圖 52 所示，56% 的警示受過調查，44% 則並未調查；而在這些受過調查的警示中，28% 被視為合理的警示。46% 的合理警示隨後已經修復。

以具體的數字說明這個問題，假設組織每天記錄到 5000 個警示，意味著：

- 2800 個警示 (56%) 受過調查，而 2200 個警示 (44%) 並未調查
- 在這些受過調查的警示中，784 個 (28%) 為合理警示，而 2016 個警示 (72%) 不是
- 在這些合理的警示中，360 個 (46%) 已經修復，而 424 個警示 (54%) 並未修復

將近半數的警示沒有調查，這一點應值得注意。到底是哪些警示沒有修復：是只會散佈垃圾郵件的低階威脅嗎？還是可能導致勒索軟體攻擊或癱瘓網路的威脅呢？若要更宏觀地調查並瞭解威脅態勢，組織必須倚靠自動化機制和適當整合的解決方案。自動化有助於安全性團隊善用珍貴的資源，免除他們在偵測和調查上的負擔。

既然沒有能力檢視如此大量的警示，這又讓我們好奇這些警示對組織整體成功的影響：這些未經調查的威脅，對公司的工作生產力、客戶滿意度和信心程度有何影響？受訪者告訴我們，即便是小型的網路中斷或資安漏洞，都有可能對淨利造成長遠的影響。即使損失不大，且受影響的系統非常容易辨識並隔離，資安主管仍會將漏洞視為大事，因為這會對組織造成某些壓力。

壓力對組織的影響展現在多個方面。資安團隊必須在資安漏洞出現後花時間管理網路中斷，近半數的網路中斷甚至長達 8 小時。45% 的網路中斷持續 1 至 8 小時（圖 53），15% 歷時 9 至 16 小時，11% 則為 17 至 24 小時。41% 的網路中斷影響組織系統規模達 11% 至 30%。

影響：越來越多組織因漏洞而有損失

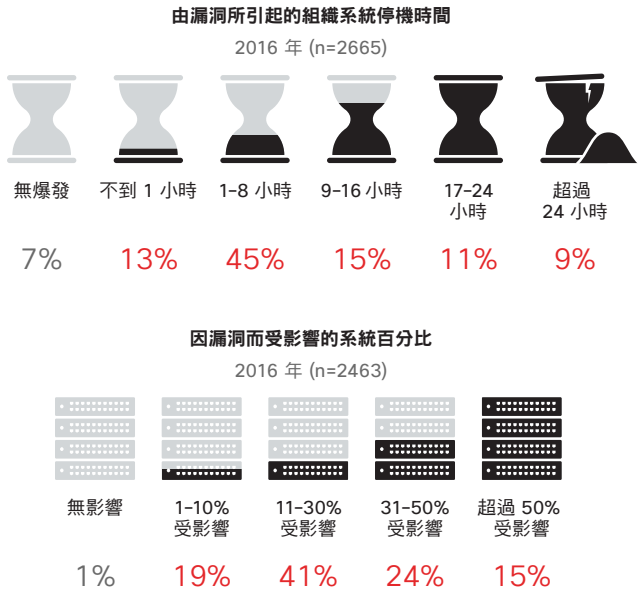
漏洞的影響不是只有網路中斷，還可能造成金錢、時間與商譽的損失。認為自己可以躲過一劫的資安團隊，其實沒有看到研究資料的現實面。我們的研究顯示，近半數的組織在資安漏洞後，還得處理大眾的檢視。有鑑於攻擊者的能力和戰術範圍，問題不再是資安漏洞是否會出現，而是什麼時候出現。

基準研究顯示，資安專業人員在發生資安漏洞時必須面對現實，因而經常變更資安策略或加強防護。而尚未受到攻擊者入侵網路的組織，可能會以為自己躲過一劫，但是他們的信心用錯地方了。

49% 的受訪資安專業人員指出，組織曾經必須處理資安漏洞後的大眾檢視。在這些組織中，49% 是自願公開資安漏洞，31% 則表示是由第三方揭露（圖 54），等於有將近三分之一的受訪組織被迫處理非自行公開的情況。顯然，私下處理漏洞的做法可能早已不復存在，現在有眾多監督機關、媒體和社群媒體的使用者會將事實公諸於世。

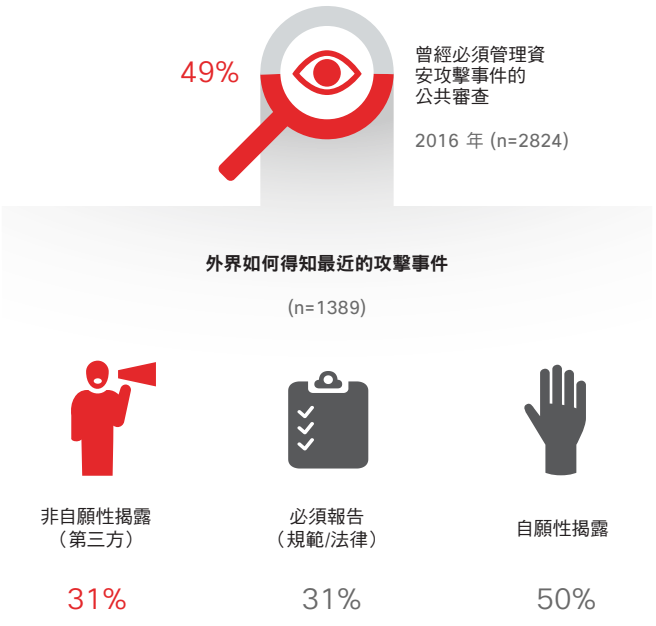
分享

圖 53 由資安漏洞引起之營運中斷的時間長度和程度



資料來源：思科 2017 年資安能力基準研究

圖 54 遭遇公共漏洞的組織百分比



資料來源：思科 2017 年資安能力基準研究

圖 55 最有可能受到公共漏洞影響的功能

資料來源：思科資安研究部門

分享

組織遭受的損失遠遠大於處理漏洞或中斷所投入的時間，企業應該極力避免如此實質且重大的影響。

如圖 55 所示，36% 的資安專業人員指出，營運是最有可能受到影響的部門。這意味著，影響交通、醫護和製造等眾多產業的核心生產力系統，會因此減慢速度或甚至停機。

財務部門則排在營運之後（30% 的受訪者表示其最可能受到影響），再來是品牌信譽和客戶維繫（兩者同為 26%）。

沒有任何一家希望成長及成功的組織，願意冒著重要部門受到資安漏洞影響的風險。因此，資安專業人員在檢視這份調查結果時，應回頭觀察自己的組織並捫心自問：如果我的組織因為漏洞而遭受這樣的損失，這對公司未來的營運會造成什麼影響？

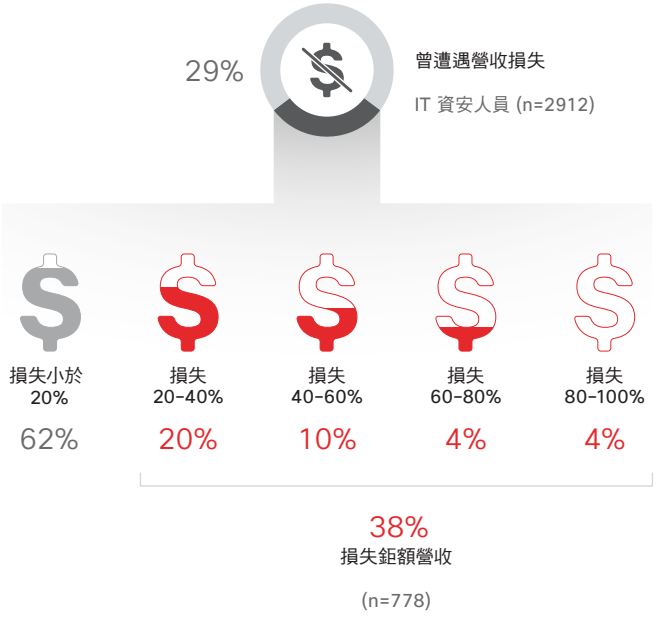
公司因為線上攻擊而損失商機，這無非是令人氣餒的事情。23% 的受訪資安專業人員指出，他們的機構在 2016 年曾因為攻擊而損失商機（圖 56）。在這些人之中，58% 表示損失的商機總計低於 20%，25% 認為有 20% 至 40%，9% 則回答 40% 至 60%。

多數組織可以量化資料外洩所致的營收損失。如圖 57 所示，29% 的資安專業人員指出，組織曾因攻擊而有營收損失的情形。在這些人之中，38% 表示損失的營收大於 20%。

網路攻擊也可能造成客戶流失。如圖 58 所示，22% 的組織表示曾因為攻擊而流失客戶。在這些組織之中，39% 表示流失的客戶大於 20%。

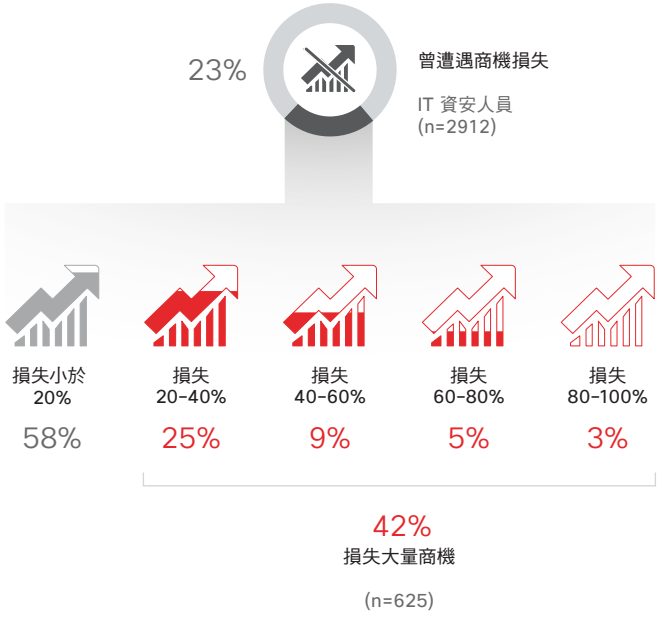
下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

圖 57 因受到攻擊而損失的組織營收百分比



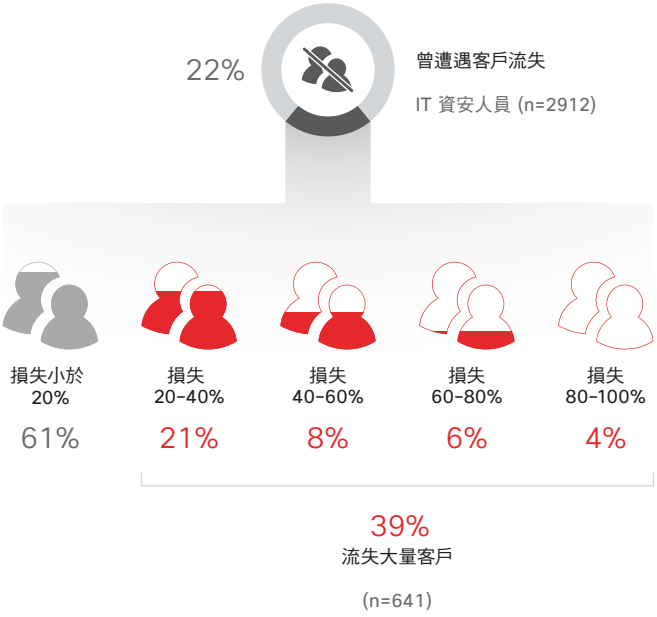
資料來源：思科 2017 年資安能力基準研究

圖 56 因受到攻擊而損失的商機百分比



資料來源：思科 2017 年資安能力基準研究

圖 58 公司因受到攻擊而失去的客戶百分比



資料來源：思科 2017 年資安能力基準研究

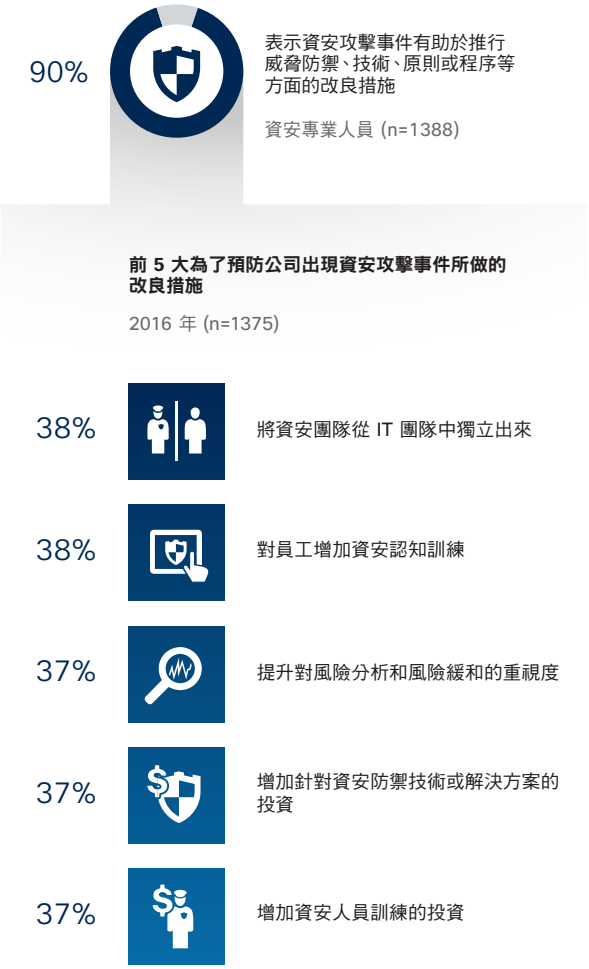
結果：擴大審查在資安改良措施中扮演重要角色

調查結果顯示，漏洞影響的範圍可能既久又廣。假設組織會在某天受到漏洞影響，問題就在於後續的情形會是如何？管理階層應將注意力和資源轉至何處，才能降低類似漏洞的可能性？

漏洞的後續影響是一個學習的機會，必須利用這個經驗來投資更好的做法。

90% 的資安專業人員指出，資安漏洞曾促使威脅防禦技術和程序的改進，如圖 59 所示。在曾經受到漏洞影響的組織中，38% 表示他們的應變方式是將資安團隊從 IT 部門獨立出來，38% 增加員工的安全認知訓練，另有 37% 則是加強風險的分析和降低。

圖 59 資安漏洞如何促進改善措施的推行



資料來源：思科 2017 年資安能力基準研究

組織開始明白需要運用創意，才能克服人才、技術相容性和預算的限制。採用委外服務便是其中一個策略，可以加強預算的控制，還能善用外部的人才。

在 2016 年，51% 的資安專業人員將建議與諮詢委外處理，45% 則將事件回應委外（圖 60）。52% 的受訪者表示委外服務可以節省成本，48% 的受訪者則認為可以藉此獲得公正的分析。

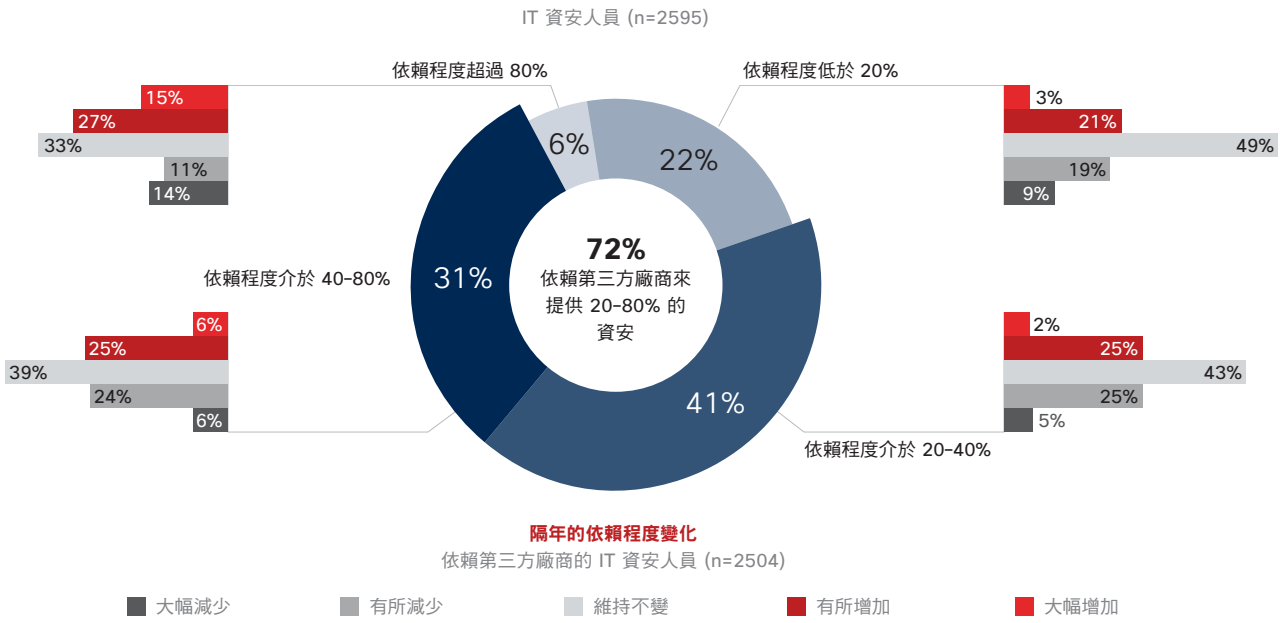
除了委外之外，組織也仰賴第三方廠商來加強防禦策略，安全性生態系統使雙方可以共同承擔資安責任。

72% 的資安專業人員指出，他們有 20% 至 80% 的資安仰賴於第三方廠商，如圖 61 所示。這些高度依賴外部資安協助的組織，最常表示自己未來會增加第三方廠商的運用。

圖 60 組織對委外的依賴

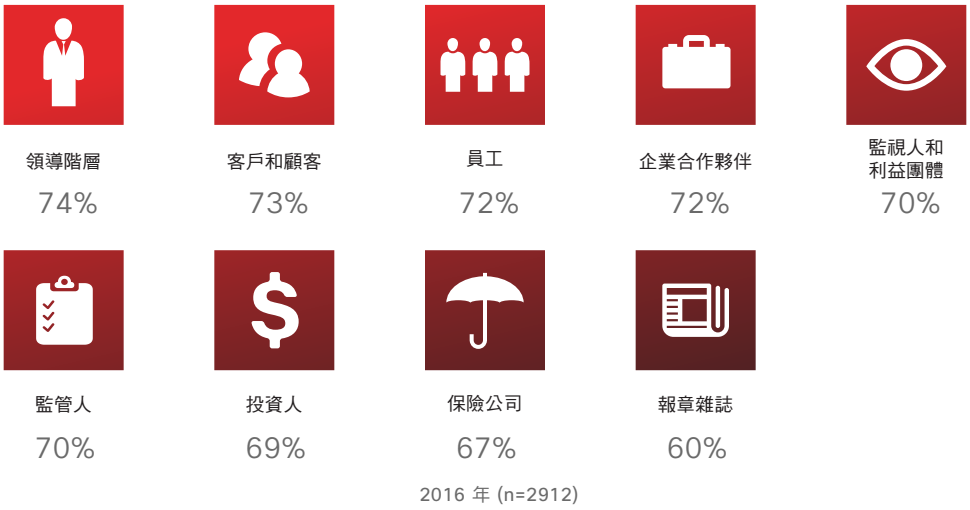
資料來源：思科 2017 年資安能力基準研究

圖 61 組織對委外的依賴程度百分比



資料來源：思科 2017 年資安能力基準研究

圖 62 擴大審查的來源

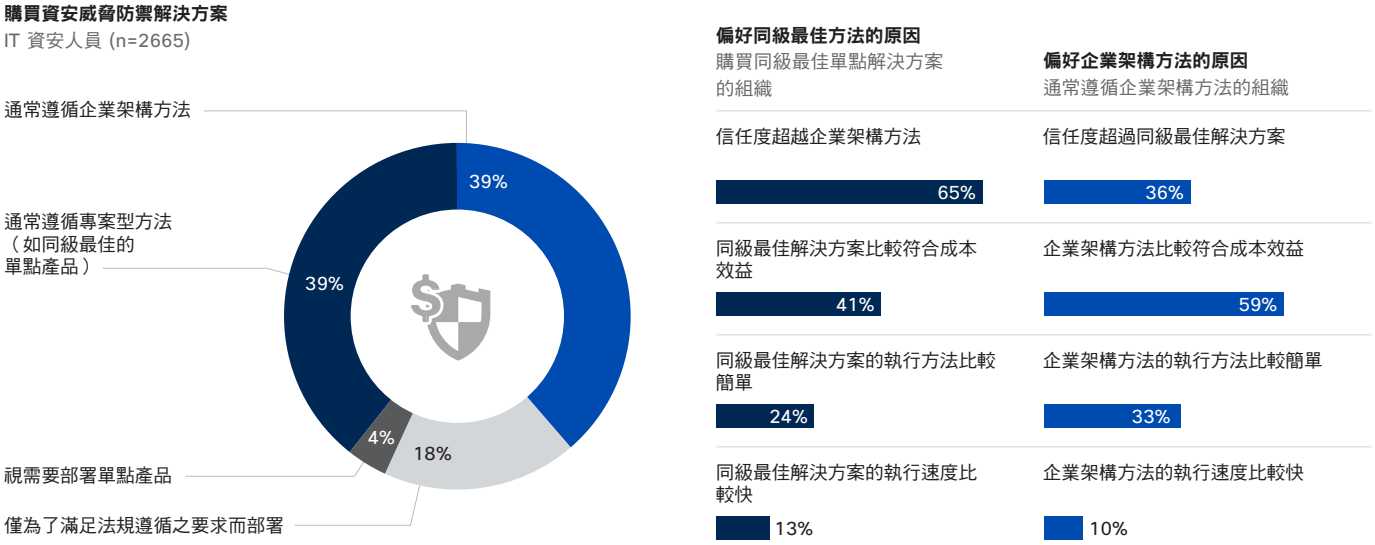


資料來源：思科 2017 年資安能力基準研究

隨著組織積極強化安全性態勢，想必他們的付出也會因此受到更多的關注。這樣的監督來自具有影響力的人士，因此不能輕易忽視。該如何解決這些人士的擔憂，對組織的自保能力有很大的影響。

74% 的資安專業人員指出，監督來自領導階層主管；73% 來自客戶和顧客，而 72% 則來自員工，如圖 62 所示。

圖 63 信任和成本節約效益如何有助於制訂資安決策



資料來源：思科 2017 年資安能力基準研究

信任與成本：什麼因素驅使公司採購資安商品？

資安專業人員無非希望能以最好的解決方案保護組織，但是他們對如何建立理想的安全環境卻有不同的看法。他們是因為相信某些解決方案可以解決各種不同的問題，而從眾多廠商之中選出最好的解決方案嗎？還是因為相信某個做法比較符合成本效益，轉而選擇整合式架構呢？投資資安的動機固然很多，但更簡便的解決方案才能有利於每個組織。

如圖 63 所示，資安專業人員對於信任與成本的選擇似乎不相上下，選擇最佳解決方案和架構型解決方案的比例相同。65% 的受訪者表示，他們之所以選擇最好的解決方案，是因為他們比較不相信企業架構模式。另一方面，59% 則認為架構模式較符合成本效益而加以選擇。

這不是一個非黑即白的問題，組織同時需要最好和整合的資安解決方案。兩種模式各有優點，可以簡化資安作業，同時提供自動化的應變工具（圖 63）。

若能將最好和整合的解決方案結合，資安團隊必能降低資安作業的複雜度，又可增加作業效率。整合的做法有助於資安專業人員瞭解各防禦階段的情況，進而限縮攻擊者的操作空間。這種做法簡單，有利於團隊大規模部署解決方案；這種做法開放，有助於選出所需的最佳解決方案；另外，自動化的特點更可加快偵測作業。

結論：基準研究透露的訊息

為了降低風險及限制惡意人士的操作空間，增加安全性工具和真有能力運用這些工具，是兩個完全不同的事情。基準研究的受訪者自認擁有可以擊退攻擊者的工具，但是他們也承認，由於缺少人力和產品相容性不佳等限制因素，再好的工具也無法發揮符合預期的效果。

這些與漏洞影響有關且發人省思的發現，適足以向安全性工具專業人員證明，改善程序和通訊協定的必要性。面對營收損失和客戶流失如此真實且立即的影響，組織不能再只是希望安全防護沒有紕漏就好，因為重點不在於漏洞是否會出現，而是遲早會出現的問題。

基準研究透露出一個訊息：我們必須永遠面對導致資安敏捷度和成效減低的限制因素，畢竟預算和人才始終不如安全性工具專業人員的預期。如果可以接受這些限制，就不難想出簡化資安作業及部署自動化解決方案的做法。

簡化資安作業時，可以利用最佳解決方案和整合型架構，兩種做法對組織而言各有好處。

產業

產業

價值鏈安全性：數位世界的成功取決於能否減輕第三方的風險

在這個牽一髮而動全身的經濟中，價值鏈安全性可以說是成功的必要條件，必須確保整個價值鏈，即軟硬體和服務從頭到尾的生命週期，都有場合及時機正確的適當安全機制。

價值鏈的八個階段如圖 64 所示。

在數位化的世界中，資訊科技和運營技術已經密不可分。組織不能只想著要保護內部商業模型、產品服務和基礎架構，而是要以全面的角度檢視價值鏈，考慮每個參與商業模型或接觸產品服務的第三方，是否會對資安造成風險。

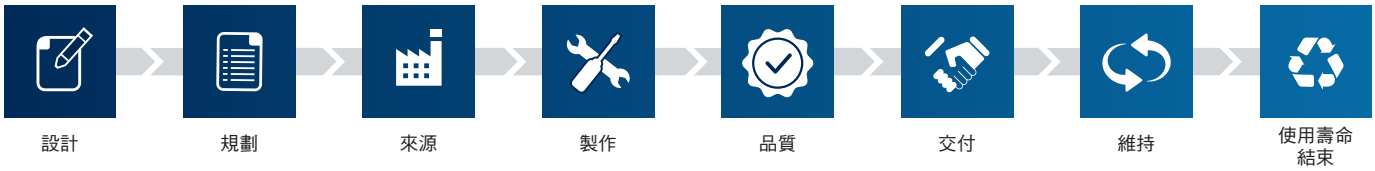
簡單來說，任何第三方都可能有風險：SANS 協會的研究指出，80% 的資料外洩都是第三方所致。[15] 如果想要降低風險，組織的價值鏈就不能全然信任他人，且資安是每個人的責任。朝著這個目標跨出第一步時，企業應該：

- 找出第三方生態系統中的關鍵角色，瞭解這些第三方提供的服務為何
- 開發一個彈性的安全性架構，可在生態系統的眾多第三方之間共用及部署
- 評估這些第三方的運作是否介於組織安全性架構所訂的容許範圍內
- 在數位化程度增加的同時，密切注意生態系統可能造成的新資安風險

在採用新的商業模型或產品服務，且會因此需要或影響第三方的生態系統之前，組織也必須考慮到安全性。任何可能的價值及生產力提升，都必須和潛在的風險兩相權衡，特別是資料安全和隱私。

對價值鏈的重視，在全球和特定產業中都有普及的趨勢。美國最近通過的 IT 採購法授權國防部，得針對資訊科技和網路安全的採購案，進行為期一年的開放技術標準評估。[16] 在高度聚集的能源產業中，北美電力可靠度公司 (NERC) 也正在積極制訂有關網路價值鏈的新規定。[17]

圖 64 價值鏈的階段



資料來源：思科

分享

[15] *對抗供應鏈中的網路風險*，SANS Institute，2015：https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252。
[16] 公法 114-92 §
[17] 美國聯邦能源管理委員會任命 NERC 著手進行這項工作；18 CFR Part 40 [Docket No. RM15-14-002; Order No. 829]。

組織和第三方需要共同回答若干問題，例如：「資料如何產生？由誰產生？」和「是否要以數位的方式挖掘資料？」如果想要進一步瞭解，更需要決定以下問題的答案：「誰擁有我們正在收集或建立的數位資產?」和「我們必須和誰分享這些資訊？」另外還有一個重要的問題需要回答，那就是：「出現漏洞時，誰必須負起什麼樣的責任和義務？」

這種以價值鏈為中心的做法，有助於確保資安的考量融入解決方案生命週期的每一個階段。若能建立正確的架構，加上遵守相關的安資安標準，必能在整個價值鏈中創造全面的安全與信任。

地緣政治的最新動態：加密、信任和透明度要求

在先前的網路安全報告中，思科的地緣政治專家曾討論過：網際網路管理環境中的不確定性、個人權利和國家權利的取捨，以及政府及私人企業如何克服資料保護的難題，而「加密」是這些討論的共同主題。我們相信在不久的將來，「加密」此一主題仍可見於（甚至是主導）有關網路安全的討論。

國家與區域的資料隱私法規與日俱增，已經讓各家廠商和使用者感到不安，無不試圖度過這些法規的難關。在這種不確定的環境中，資料主權和資料在地化等成了必須解決的首要議題，而這也帶動了雲端運算和在地化資料儲存的成長，畢竟企業都在尋找創新的解決方案，以符合複雜又不斷變化的隱私法規。[18]

與此同時，資料外洩和進階持續性威脅的問題層出不窮，以及由民族國家出資的駭客活動時有所聞（例如：在美國總統大選等受到高度矚目的活動期間，曾經發生駭客活動），這些更讓使用者再度失去信心，懷疑自己的敏感資料和隱私權是否真能受到保護。

「後史諾登」時代的政府越來越堅持，要在需要時管理數位通訊及存取資料，但使用者也積極爭取自己的隱私權。Apple 和 FBI 日前還為了恐怖份子持有的 iPhone 而正面交鋒，這類的事件對消弭使用者的隱私權疑慮更是毫無幫助。如果真有什麼幫助，大概也是讓數位時代的使用者（特別是美國），瞭解到什麼是端對端加密。許多使用者開始會要求技術供應商提供端對端加密，而且他們希望自行保管加密金鑰。

這種現象在根本上改變了我們所認知的網路安全情勢。現在組織架構的環境，必須幫助他們克服及因應相互衝突的的議題。

在這種改變發生的同時，也有越來越多政府讓自己有權（且常是廣泛的權利），繞過或破解加密或技術保護措施，而且通常不需知會製造商、通訊業者或使用者。這不僅會造成主管機關和科技公司之間的對立，甚至會讓政府之間的關係更趨緊張，畢竟不是所有政府都希望看到，公民的資料遭到第三國家機關存取。許多政府都會收集廠商軟體中零時差攻擊和弱點的相關資訊，卻不一定會和廠商表明自己擁有哪些資訊，或者與廠商即時分享資訊。

「私藏」這些重要資訊，會使廠商無法提升產品的安全性，以及為使用者提供更好的威脅防護。即便政府可能有正當的理由保密部分情報，但在全球化的網路安全環境中，還是需要更大的透明度及信任。因此，政府應就目前潛藏著零時差攻擊的各項政策，坦誠地進行評估。首先要讓一切回歸原點，相信與廠商分享資訊只會有利無害，為所有人創造一個更安全的數位環境。

[18] 如需該主題的詳細資料，請參閱「法規不確定性未能解決，資料在地化鬆綁」，Stephen Dockery，2016 年 6 月 6 日，*The Wall Street Journal*：http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/。

高速加密：保護傳輸中資料的可擴充解決方案

如同第 65 頁之地理政治一節所述，端點對端點加密仍然是造成政府與產業間針對可預見之未來爭論不休及戒慎恐懼的議題。姑且不論這個議題引發何種緊張局面，使用者對於客戶持有金鑰形式之端點對端點資料加密的需求日益增加。

根據思科地理政治專家的預測，某些資料串流和集區在短期內依然會經過由廠商所管理的金鑰加密，而廣告導向的商業模式尤其如此。另一方面，我們應該能預期使用客戶持有金鑰形式之端點對端點加密會造成更強烈的摩擦，原因在於缺少約束反對方的法律命令。

在此同時，設法進一步控制傳輸中資料之保護方式（特別是從某資料中心高速移動到另一個資料中心）的組織，也值得我們關注。由於傳統技術的限制和影響網路效能甚鉅等因素，這項工作曾是企業難以實現的目標。然而隨著新方法的問世，這項工作的程序也獲得簡化。

其中一個解決方案是應用程式層安全性，亦即藉由修改應用程式來為資料加密。組織使用的應用程式數量不盡相同，部署這類安全性可能需要耗費大量資源、執行方式複雜且營運成本昂貴。

另一個引發摩擦的方法，是將加密功能內建於網路或雲端服務中，進而保護傳輸中的資料。這個解決方案是傳統閘道 VPN 模式的進化版，它能迎合網路不斷變動的本質，以及資料中心流量的急遽傳輸速率。企業正運用新功能帶來的營運和成本節約效益來保護該環境內由任何應用程式產生的資料，護送它們高速移動到其他位置。

即便如此，以網路為基礎的加密機制只能算是一種保護資料的工具。若要確保它們足以保護傳輸中或靜止的資料，組織應將他們所面臨的挑戰納入全面性考量。向技術廠商提出基本但重要的問題是個不錯的起點，例如：

- 資料傳輸時的保護方式為何？
- 資料靜止時的保護方式為何？
- 誰擁有資料的存取權限？
- 資料的存放位置為何？
- 當/假設資料必須刪除時，資料的刪除原則為何？

再次強調，這些問題只是激發更廣泛之資料保護對話，涵蓋如資料恢復力和可用性等主題探討的起點。

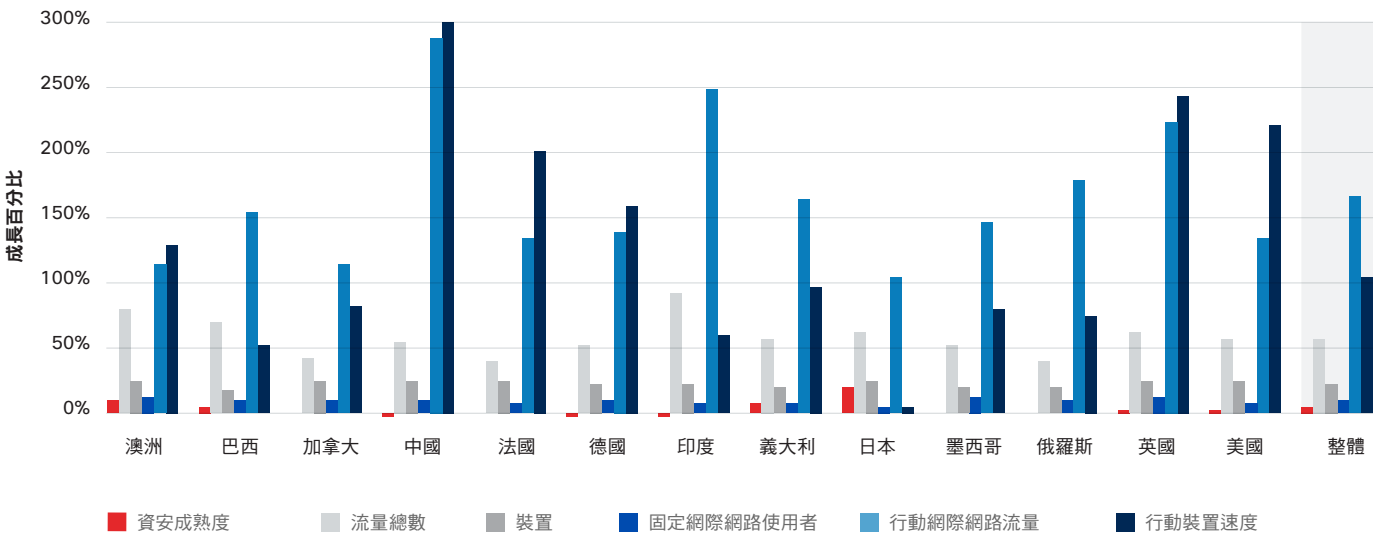
網路效能和採用 vs. 資安成熟度：線上速度、流量和準備程度並未同步成長

防禦者希望能在惡意人士之前先發制人，因為只要稍一落後，就有可能處於險境。然而，問題就在於防禦者改善其資安態勢的步調，不及惡意人士進行操作的空間與時間。有鑑於全球固定和行動網際網路流量的成長速度，防禦者只能順應這樣的成長步調，來提升安全性基礎架構的成熟度。

思科 VNI 預測每年都會檢查全球 IP 流量（包括行動網路與 Wi-Fi 流量），預測未來 5 年內的 IP 流量、網際網路的使用者數量，以及 IP 網路支援的個人裝置和機器對機器 (M2M) 連線數量。（如需 VNI 預測的詳細資料，請前往此處。）舉例來說，預測指出在 2020 年以前，智慧型手機會佔 IP 總流量的百分之三十。

思科曾將 VNI 預測對應至防禦者成熟度的資料（取自思科年度資安能力基準研究，請參閱第 49 頁），並在檢視 2015、2016 和 2017 年基準報告的成熟度成長率（如圖 65 所示）時，發現資安成熟度遠不及網際網路流量的成長速度。在這段期間內，某些國家/地區（如中國和德國）甚至還有成熟度稍退的現象。圖 65 中尤其值得注意的是，寬頻速度的改進和成長率遠遠超過其他網路形式。速度的提升和連線裝置的增加，帶動了更大的流量成長，但是組織卻很難以相同的步調加強安全措施和基礎架構。

圖 65 資安成熟度和成長率



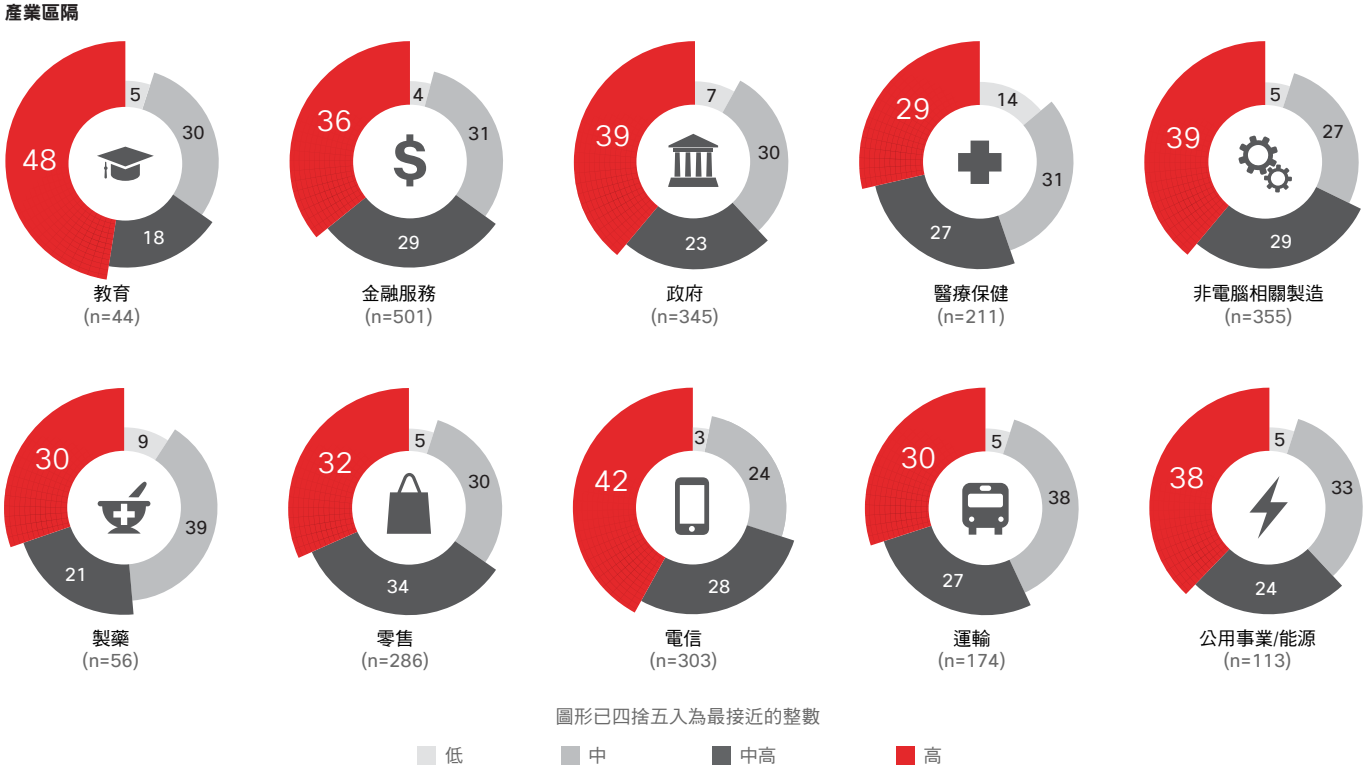
資料來源：思科資安研究部門、思科 VNI 及思科 2017 年資安能力基準研究

在資安成熟度方面，某些產業甚至更為落後（如圖 66 所示），如製藥、醫護和交通產業的流量尤其如此。

值得注意的是，行動網路速度的大幅成長，是因為電信業者大幅採用 4G 和 LTE 網路所致。如果在 2020 年以前可以大規模部署 5G 網路，行動網路的速度可望能與固定網路衡。最新的行動網路 VNI 預測指出，未來大規模採用 5G 後，全球行動網路流量將有可能在 IP 總流量中佔更大的比例。根據 VNI 預測，全球行動網路流量在 2015 年共佔 5% 的 IP 總流量，而預計會在 2020 年達到 16%。

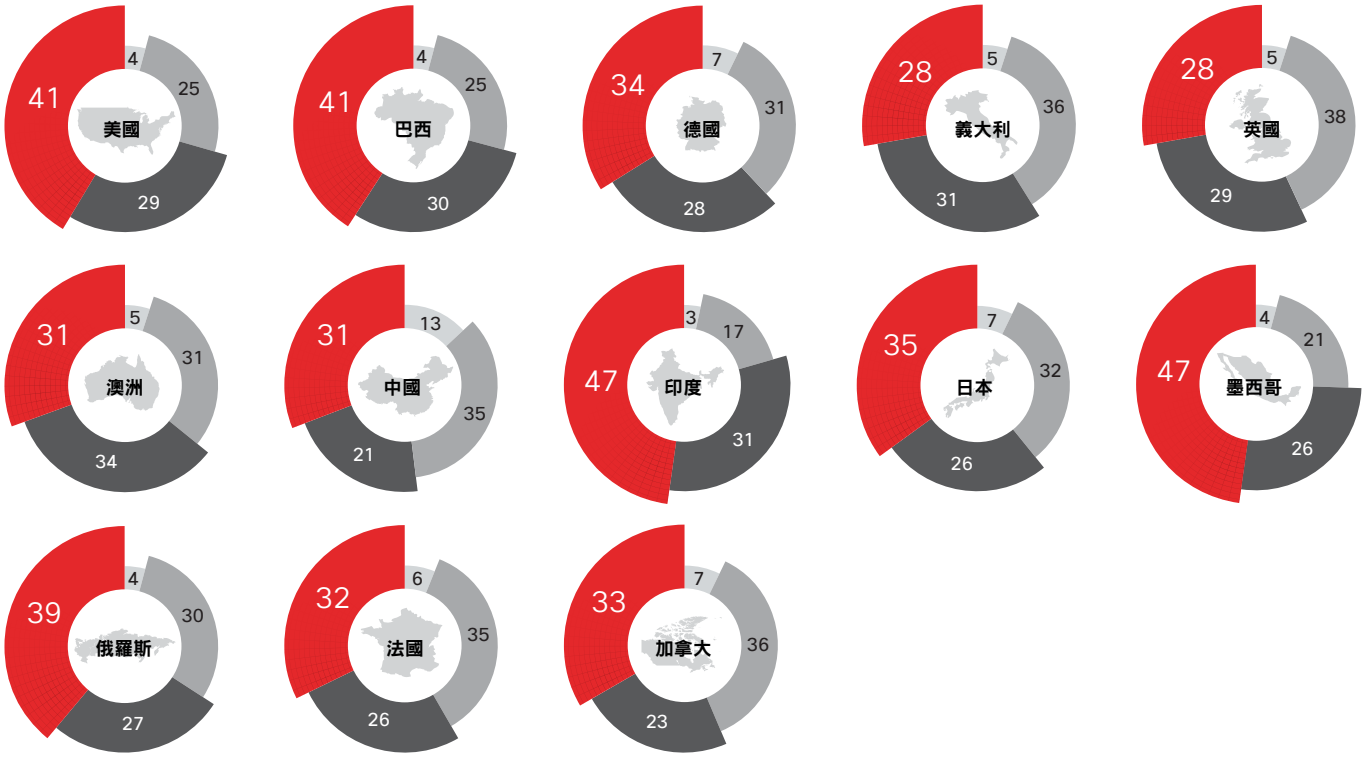
顯然，資安組織如果想要跟上網際網路流量的成長，避免受到隨之而來的潛在攻擊範圍擴大影響，就必須加緊腳步增加成熟度。此外，隨著企業網路的非固定和無線連線端點日益普及，組織也必須訂有對策，更需要因應越來越多員工透過個人裝置存取公司資料的情況。

圖 66 垂直產業中的資安成熟度



資料來源：思科 2017 年資安能力基準研究

圖 67 依據國家排列的資安成熟度



資料來源：思科 2017 年資安能力基準研究

速度提升並非網際網路流量成長的唯一因素。IoT 更是增加網際網路連接裝置的成長速度，這雖然帶動了流量的提升，卻也增加攻擊者的入侵機會。

如需關於思科 VNI 預測的更多資訊，請前往思科網站，或閱讀關於2015 年至 2020 年年度 VNI 預測的思科部落格文章。

結論

結論

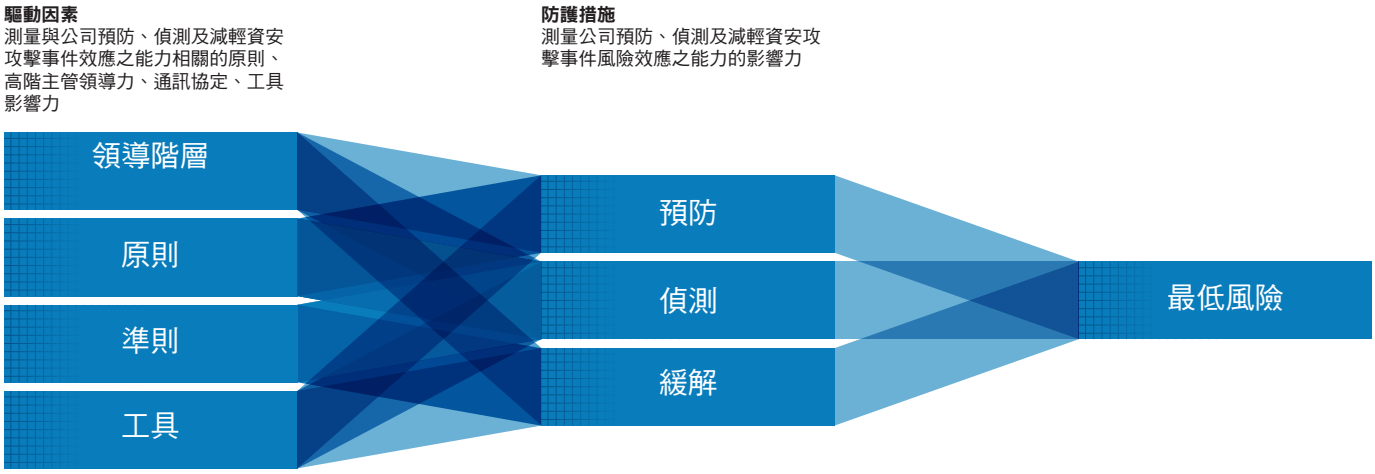
隨著攻擊範圍的迅速擴張，資安需採取互連且整合的做法

藉由思科資安能力基準研究（請參閱第 49 頁）的資料分析，我們可以檢視有助於組織大幅降低風險的各種模式和決策，從中瞭解他們應在哪些方面挹注安全性資金，才能讓自己在風險暴露的領域中脫穎而出。我們在評估風險時，是以漏洞長度和系統中斷的比例計算（請參閱第 55 頁圖 53，瞭解何謂漏洞長度和受影響系統）。

為瞭解組織如何針對風險進行有效的防禦，我們需要檢視哪些因素會影響他們的風險預防、偵測和降低能力。（請參閱圖 68）。這些因素必須包含以下要素：

- **領導階層主管：**最高領導必須將資安視為優先要務，這對攻擊的風險降低和預防而言非常重要。執行團隊還應針對安全性計畫的成效，訂定清楚且明確的評估指標。
- **政策：**政策與風險降低息息相關。網路、系統、應用程式、功能和資料的存取權控制，會決定是否有能力減輕資安漏洞所致的損壞。此外，訂有安全措施的定期檢查政策，也有助於預防攻擊事件。
- **通訊協定：**正確的通訊協定有助於預防及偵測漏洞，不過其與風險降低也有密切關係。具體而言，定期檢查網路上的連線活動，除了確保安全措施正常運作外，更是風險預防和降低的關鍵所在。此外，持續定期、正式且策略性地檢查並改善安全措施，也有立竿見影之效。
- **工具：**明智且適當地應用工具，這與風險降低的關係最大。如果擁有合適的工具，使用者便能檢查及提供重要的意見，有利於風險的偵測、預防和降低。

圖 68 降低風險的驅動因素和防護措施



資料來源：思科 2017 年資安能力基準研究

下載 2017 年圖表：**www.cisco.com/go/acr2017graphics**

組織使用的安全防護措施，包括預防、偵測與降低，也會影響組織降低風險的能力。（請參閱圖 68。）

這些防護措施必須包含以下要素：

- **預防：**為將資安漏洞的影響降到最低，員工必須回報任何安全錯誤和問題。此外，安全性程序和流程也應該清楚明瞭。
- **偵測：**一個能有效降低漏洞影響的最佳偵測方法，必須讓組織能在資安弱點演變為完整事件之前時加以察覺。為此，必須針對事件相關資訊訂有良好的分類制度。
- **降低：**針對事件的應變和追蹤確立相關程序和流程，這對資安漏洞的風險降低而言相當重要。組織也應訂有強大的通訊協定，藉此管理危機的應變處理。

這些因素和防護措施牽一髮而動全身，資安專業人員不能只是挑選幾個因素，以及一兩種防護措施，就斷然相信安全問題已經解決。各種因素和防護措施缺一不可，資安團隊必須分析自己的弱點，例如：領導階層給予的支持不足，或缺少降低漏洞風險的工具，再來評估應在何處進行資安投資。

關鍵目標：減少惡意人士的操作空間

減少惡意人士不受約束的操作空間（最好能完全消除）並掌握攻擊者的目前狀態，才是防禦者的首要優先要務。事實上，沒有人能夠阻止所有的攻擊，或者完全保護可以也應當保護的事物。不過，如果將焦點放在縮減網路罪犯的操作空間，讓他們無法進行有效且可從中獲利的活動，便能防止他們完全躲過偵測，而侵入重要的系統和資料。

本報告針對惡意人士危害及攻擊使用者和系統的方法進行分類。偵察、武器化、派送和安裝等四個類別，係依據其在攻擊鏈中典型的部署階段而定，旨於說明惡意人士利用漏洞和其他弱點的時機、方法和位置，瞭解他們如何入侵裝置或系統、發動攻擊活動並收割成果。

我們建議防禦者隨時調整安全措施，才能在攻擊者的基本程序之前做足準備。例如，若要在偵察階段消弱惡意人士，資安團隊應該：

- 收集最新威脅與弱點的相關資訊
- 確實控制網路的存取權
- 降低組織面對攻擊範圍擴大的風險
- 管理組態設定
- 針對偵察手法，制定一致的應變措施和程序

當攻擊者派送武器化的威脅時，防禦者必須善用手中的每一個工具，極力避免威脅擴散和惡化。此時，整合式安全架構遂扮演舉足輕重的角色，提供的即時威脅分析，以及自動化偵測和防禦，都有利於強化威脅偵測。

在安裝階段，資安團隊必須隨時掌握環境狀態，同時針對危害進行應變和調查。如果環境簡單、開放且已自動化，防禦者又能採取上述其他步驟主動出擊，就可將資源用在協助公司回答以下重要問題：

- 攻擊者存取了什麼？
- 他們為什麼能夠得逞？
- 他們的蹤跡為何？
- 他們還在我們的網路中操作嗎？

這些問題的答案不僅可讓資安團隊採取適當的行動來預防未來的攻擊，更能向管理團隊和委員會告知可能暴露於風險之中和必須進行公開說明。接著，公司便可啟動相關程序，確保公司能全盤掌控和降低風險，以解決任何在危害期間找到的資安縫隙（即可讓惡意人士有操作空間的弱點，以成功進行攻擊）。

關於思科

思科為世界帶來智慧型網路安全防禦機制，提供業界最完整的進階威脅防護產品組合解決方案，足以應付各式各樣的攻擊向量組合。思科以威脅為中心的安全性操作方法可以有效降低複雜性和分割程度，同時提供優異的能見度、持續控制效果，以及在攻擊前、中、後期提供進階的威脅防護功能。

思科綜合安全情報 (CSI) 生態系統的威脅研究人員在單一傘下，使用取自世界各地裝置及感應器的遙測資料、公私部門的資訊，以及開放式來源社群內容，整合了業界頂尖的威脅情報。這些情資包含每日擷取的數十億個網路要求，以及數百萬封電子郵件、惡意軟體範例以及網路入侵事件。

我們精密的基礎架構與系統會吸收這些遙測資料，協助機器學習系統和研究人員在各大網絡、資料中心、終端、行動裝置、虛擬系統、網頁、電子郵件以及雲端追蹤威脅所在位置，進而確定根本原因及衡量爆發範圍。匯集的情資會轉換為我們產品及服務中的即時保護機制，並且立即傳達給我們位於世界各地的思科客戶。

若要瞭解更多有關思科的威脅中心資安方法，請造訪 www.cisco.com/go/security。

思科 2017 年度網路安全報告投稿人

CloudLock

思科旗下公司 CloudLock 為雲端存取安全代理 (CASB) 解決方案的領先供應商，專門協助企業組織以安全的方式使用雲端。CloudLock 可以跨使用者、資料和應用程式，深入探索及控制軟體即服務 (SaaS) 解決方案、平台即服務 (PaaS) 和基礎架構即服務 (IaaS) 環境。CloudLock 設有由資料專家主持的 CyberLab，以及群眾集思廣益的安全分析，可以提供確實可行的網路安全情報。如需更多資訊，請造訪 https://www.cloudlock.com。

安全性與信任組織

思科的安全性與信任組織強調思科的決心，亦即處理董事會及全球領導者心中最重要的兩大議題。該組織的核心任務包括保護思科公私部門客戶，實現並確保思科安全開發生命週期及信任系統可套用至思科產品與服務組合，並保護思科企業免於不斷變化的威脅。思科針對廣泛的安全性與信任採取全面性的策略，包括人員、政策、程序和技術。安全性與信任組織致力提供卓越的營運能力，並將重心放在 InfoSec、信任工程、資料保護與隱私權、雲端安全性、透明化與認證，以及進階安全性研究與政府機構。如需更多資訊，請造訪 http://trust.cisco.com。

全球政府事務

思科與各個層級的政府部門都有互動關係，主要是協助訂定支援技術部門的公共政策與法規，並協助政府達成目標。全球政府事務團隊會協助開發並影響技術相關的公共政策和法規。該團隊與產業利益關係人及相關合作夥伴協同合作，與政府領導者建立良好關係，以影響與思科業務息息相關的政策制定，及整體 ICT 的採用，以期在全球、國家及當地等層級協助政策決策走向。政府事務團隊是由前任選舉官員、國會議員、立法委員、資深美國政府官員及政府事務專家所組成，共同協助思科推廣並保護世界各地的技術使用。

認知威脅分析

思科的認知威脅分析是一項雲端服務，能透過各種網絡流量數據分析的分法，有效地發現漏洞、受保護架構內的惡意軟體，以及其他資安威脅。透過使用行為分析及異常偵測，鑑別惡意軟體感染或資料外洩的症狀，以解決邊界基礎的防禦落差。認知威脅分析仰賴進階統計模型和機械學習，以便獨立辨識新的威脅，並從中學習以及隨著時間而不斷調整。

IntelliShield 團隊

IntelliShield 團隊負責思科安全研究部門、營運部門及外部來源的弱點及威脅的搜尋、分析、整合，以及研究數據和資料之間的相互關係，進而提供 IntelliShield 安全情資服務，以支援多項思科的產品及服務。

Talos 安全情資暨研究小組

Talos 是思科的威脅情報組織，是由一群精英安全專家所組成，致力於提供思科客戶、產品和服務最完善的防護功能。Talos 是由一群頂尖的威脅研究人員所組成，他們會運用精密的系統，為思科產品建立威脅情報，以便偵測、分析及防禦已知和新興的威脅。Talos 負責維護 Snort.org、ClamAV、SenderBase.org 以及 SpamCop 的官方規則組合，同時也是思科 CSI 生態系統威脅情資的主要貢獻來源。

安全性研究及操作 (SR&O)

安全性研究及操作 (SR&O) 負責所有思科產品和服務的威脅與弱點管理，其中包括領先業界的產品安全突發事件響應團隊 (PSIRT)。SR&O 會透過不同的活動（例如思科Live 及 黑帽組織），以及透過與思科上下及同業協同合作的方式，協助客戶瞭解不斷變化的威脅環境。此外，SR&O 的創新服務包含思科的自訂威脅情報 (CTI)，可以識別尚未被現有安全性基礎架構偵測或緩解的漏洞指標。

思科視覺網路指標 (VNI)

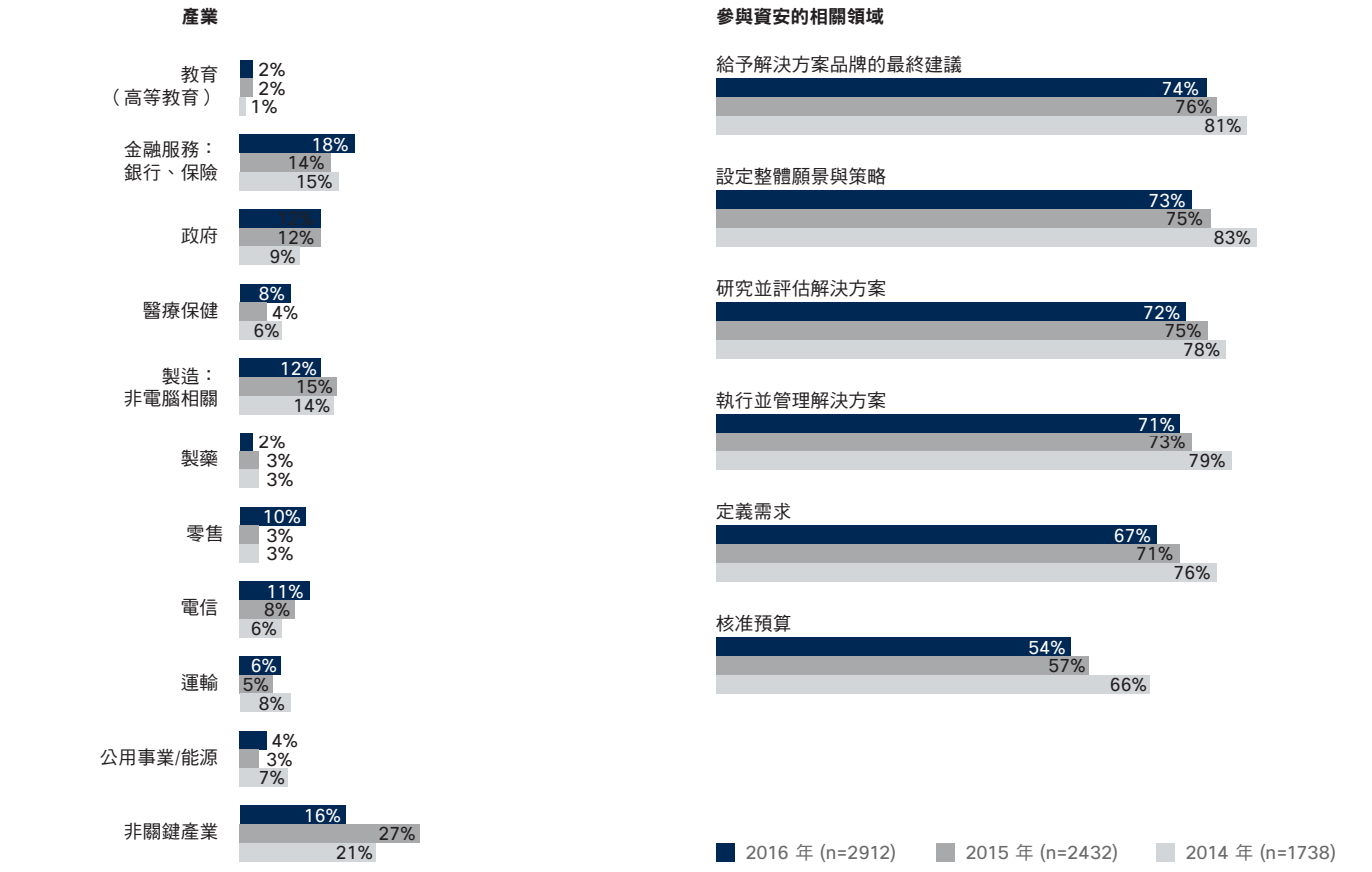
思科 VNI 全球 IP 流量預測（2015–2020 年）係以獨立分析師預測和實際網路用量資料為基礎，輔以思科本身針對全球 IP 流量和服務採用的預估。詳見完整版報告的研究方法說明。思科 VNI 研究自 11 年前首度進行以來，目前已成為各界高度認可的網際網路成長指標，許多國家政府、網路管理員、學術研究人員、電信公司、技術專家，以及工商產業的媒體和分析師，無不借助於這份年度研究報告，策劃未來的數位發展。

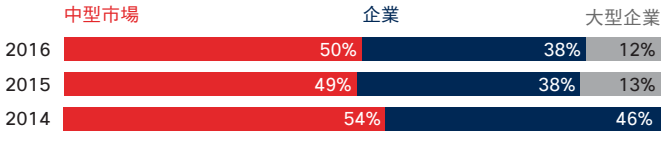
附錄

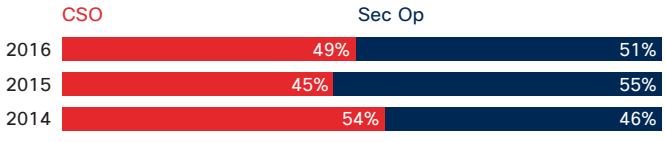
附錄

思科 2017 年資安能力基準研究

圖 69 調查能力基準研究







資料來源：思科 2017 年資安能力基準研究

圖 70 專屬資安專業人員的人數

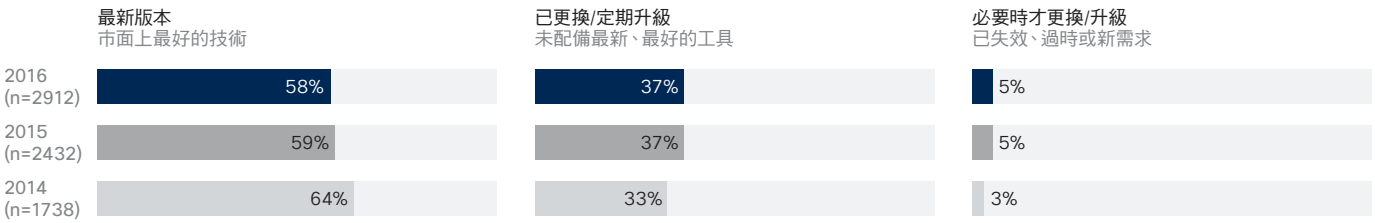
	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
200 名或更多	15%	10%	12%
專屬資安專業人員的中位數	**30**	**25**	**33**

資料來源：思科 2017 年資安能力基準研究

認知

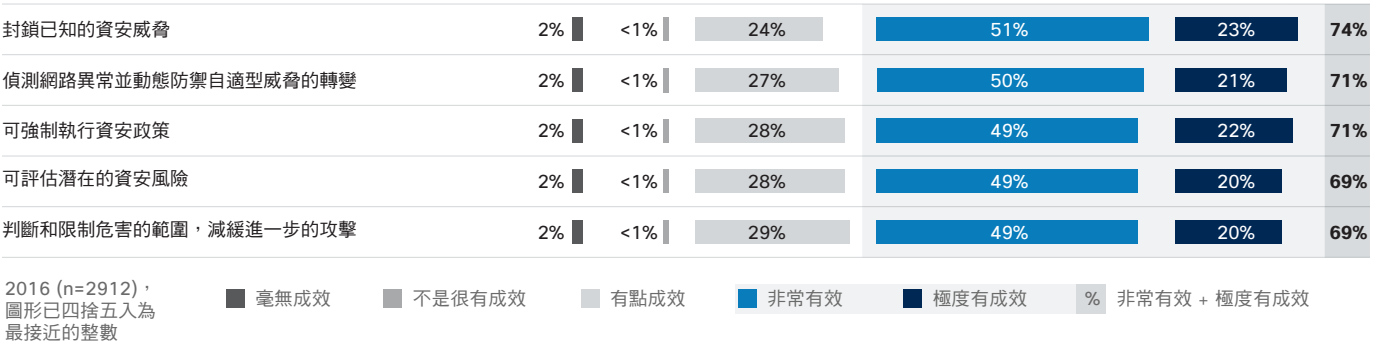
圖 71 大多數的資安專業人員認為其安全性基礎架構為最新狀態

您對您的資安基礎架構的評價為何？



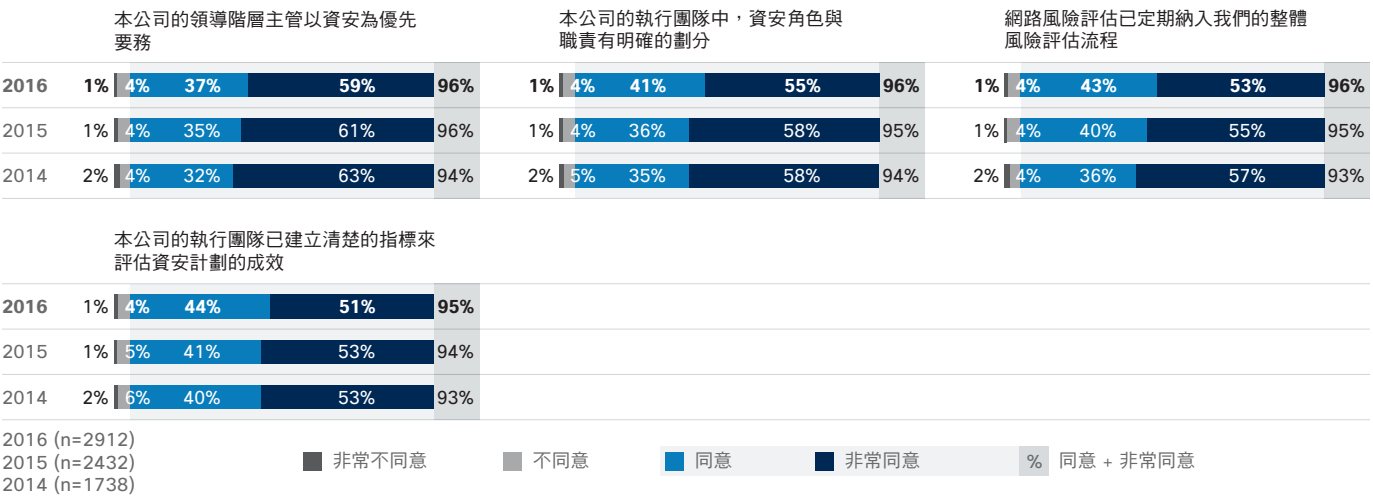
資料來源：思科 2017 年資安能力基準研究

圖 72 發現各種強效安全性工具的資安專業人員百分比



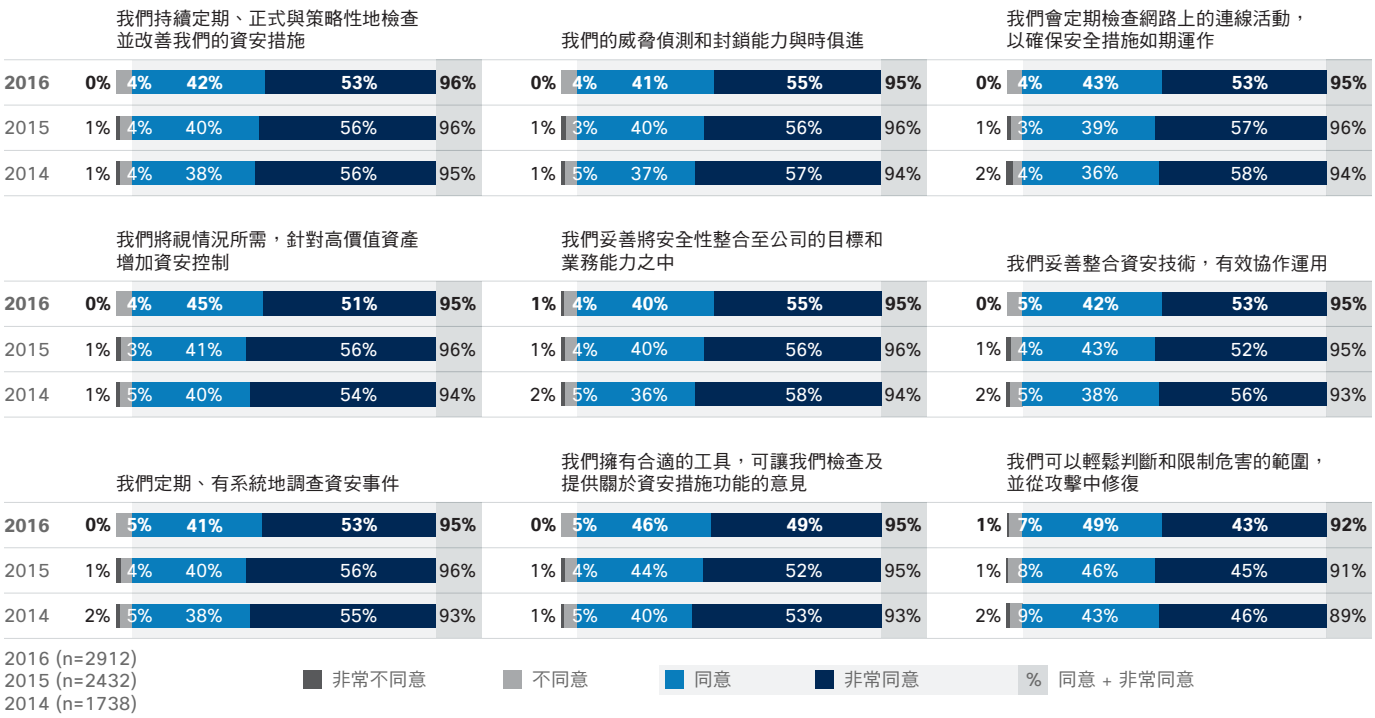
資料來源：思科 2017 年資安能力基準研究

圖 73 認為資安是經營管理層級之優先要務的資安專業人員百分比



資料來源：思科 2017 年資安能力基準研究

圖 74 非常同意安全性操作化聲明的受訪者百分比



資料來源：思科 2017 年資安能力基準研究

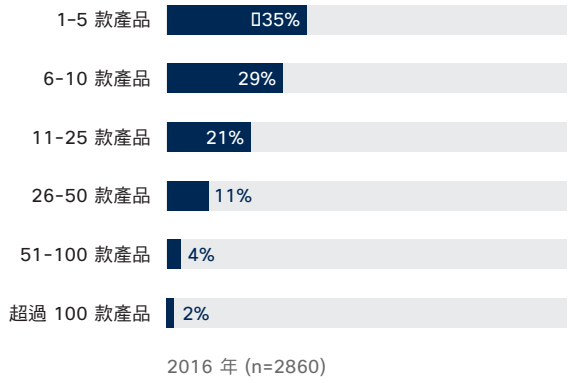
限制

圖 75 阻礙資安的最大障礙

	2015 年 (n=2432)	2016 年 (n=2912)
預算限制	39%	35%
相容性問題	32%	28%
認證需求	25%	25%
缺乏訓練有素的人員	22%	25%
競爭的優先順序	24%	24%
目前工作負載太大	24%	23%
資訊不足	23%	22%
獲市場好評後才會購買	22%	22%
企業文化/態度	23%	22%
公司不是攻擊的高價值目標	不適用	18%
資安不是經營管理層級的優先要務	不適用	17%

資料來源：思科 2017 年資安能力基準研究

圖 76 組織使用的資安廠商和產品數量



資料來源：思科 2017 年資安能力基準研究

圖 77 依據組織規模排列的使用之資安廠商數量

您的資安環境中有幾家不同的廠商（如品牌、製造商）？	中型市場 250 到 1 千名員工	企業 1 千到 1 萬名員工	大型企業 超過 1 萬名員工
1-5	46.9%	43.4%	39.9%
6-10	28.4%	30.9%	21.3%
11-20	17.6%	15.8%	23.1%
21-50	5.6%	7.1%	8.7%
超過 50	1.4%	2.8%	6.9%
組織總數	**1435**	**1082**	**333**

資料來源：思科 2017 年資安能力基準研究

圖 78 依據組織規模排列的使用之資安產品數量

您的資安環境中有幾款不同的資安產品？	中型市場 250 到 1 千名員工	企業 1 千到 10 萬名員工	大型企業 超過 1 萬名員工
1-5	37.9%	32.7%	25.1%
6-10	29.0%	30.1%	22.5%
11-25	19.8%	20.4%	23.7%
26-50	9.6%	10.5%	15.6%
51-100	3.0%	4.3%	7.8%
超過 100	0.8%	1.9%	5.4%
組織總數	**1442**	**1084**	**334**

資料來源：思科 2017 年資安能力基準研究

圖 79 IT 預算中資安預算的逐年減少程度

資安預算是否應歸在 IT 預算的一部分？（IT 部門成員）	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
全部歸在 IT 預算	61%	58%	55%
部分歸在 IT 預算	33%	33%	36%
完全獨立計算	6%	9%	9%

資料來源：思科 2017 年資安能力基準研究

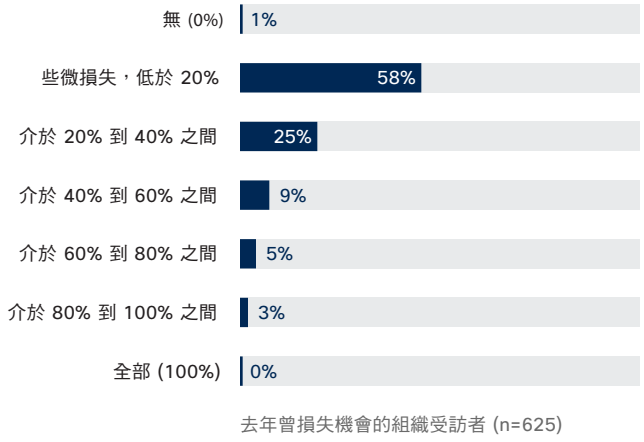
圖 80 資安支出的逐年減少程度佔 IT 預算的比率

將資安視為功能所花費的 IT 預算	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
0%	7%	9%	10%
1-5%	4%	3%	4%
6-10%	12%	11%	16%
11-15%	23%	23%	27%
16-25%	29%	31%	26%
26%-50%	21%	19%	15%
51% 或更多	5%	4%	2%

資料來源：思科 2017 年資安能力基準研究

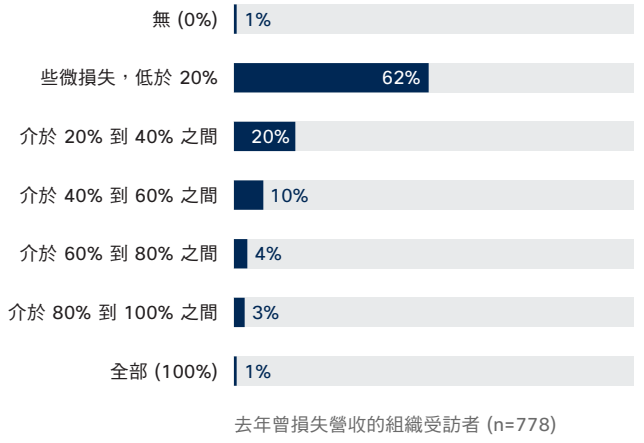
影響

圖 81 因受到攻擊而損失的組織機會百分比



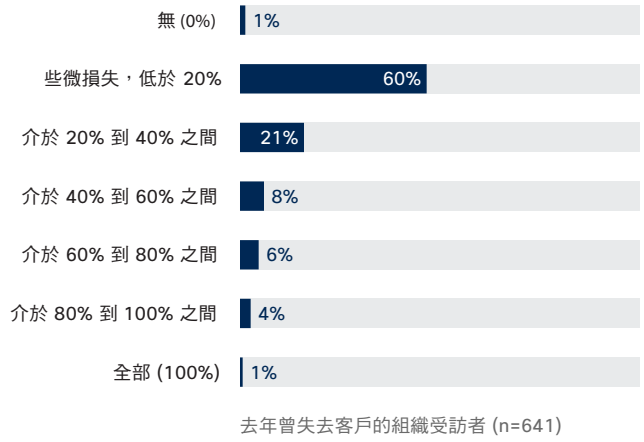
資料來源：思科 2017 年資安能力基準研究

圖 82 因受到攻擊而損失的組織營收百分比



資料來源：思科 2017 年資安能力基準研究

圖 83 組織因受到攻擊而失去客戶的百分比



資料來源：思科 2017 年資安能力基準研究

結果

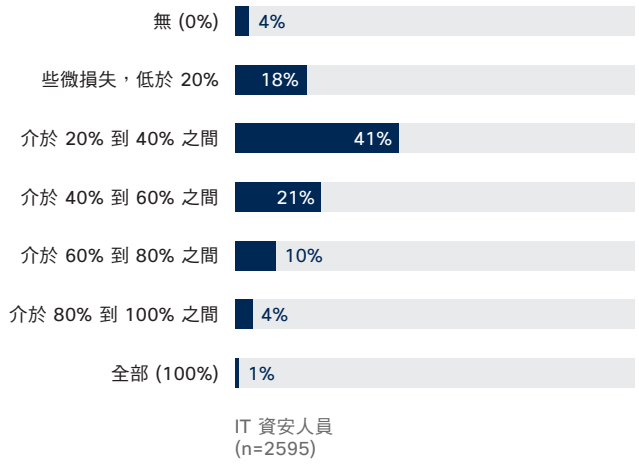
圖 84 依賴委外的組織百分比

委外的資安服務有哪些？	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
建議與諮詢	51%	52%	51%
稽核	41%	47%	46%
事件回應	35%	42%	45%
監視	42%	44%	45%
威脅情報	不適用	39%	41%
修復	34%	36%	35%
無/全部內部處理	21%	12%	10%

為何要委外這些服務？	2015 年 (n=2129)	2016 年 (n=2631)
更具成本效益	53%	52%
獲得客觀的見解	49%	48%
更即時回應事件	46%	46%
缺乏內部專業技術	31%	33%
缺乏內部資源	31%	33%

資料來源：思科 2017 年資安能力基準研究

圖 85 依賴協力廠商提供安全性的組織百分比



資料來源：思科 2017 年資安能力基準研究

圖 86 依據組織規模排列的委外資安服務百分比

委外的資安服務有哪些？	中型市場 (n=1459)	企業 (n=1102)	大型企業 (n=351)
建議與諮詢	50%	52%	51%
稽核	44%	47%	50%
監視	46%	43%	44%
威脅情報	41%	41%	40%
事件回應	48%	44%	39%
修復	35%	34%	37%
無/全部內部處理	8%	11%	11%

資料來源：思科 2017 年資安能力基準研究

圖 87 擴大審查的來源

	審查非常寬鬆	審查有些寬鬆	審查有些嚴謹	審查非常嚴謹	審查極度嚴謹	% 審查非常嚴謹 + 極度嚴謹
領導階層	2%	4%	20%	44%	30%	74%
客戶和顧客	2%	4%	21%	41%	32%	73%
員工	2%	5%	22%	44%	28%	72%
企業合作夥伴	2%	5%	22%	43%	29%	72%
監視人和利益團體	2%	5%	23%	44%	26%	70%
監管人	2%	4%	24%	43%	27%	70%
投資人	3%	5%	23%	41%	28%	69%
保險公司	3%	5%	25%	41%	26%	67%
報章雜誌	4%	8%	28%	39%	21%	60%

2016 (n=2912)，圖形已四捨五入為最接近的整數

資料來源：思科 2017 年資安能力基準研究

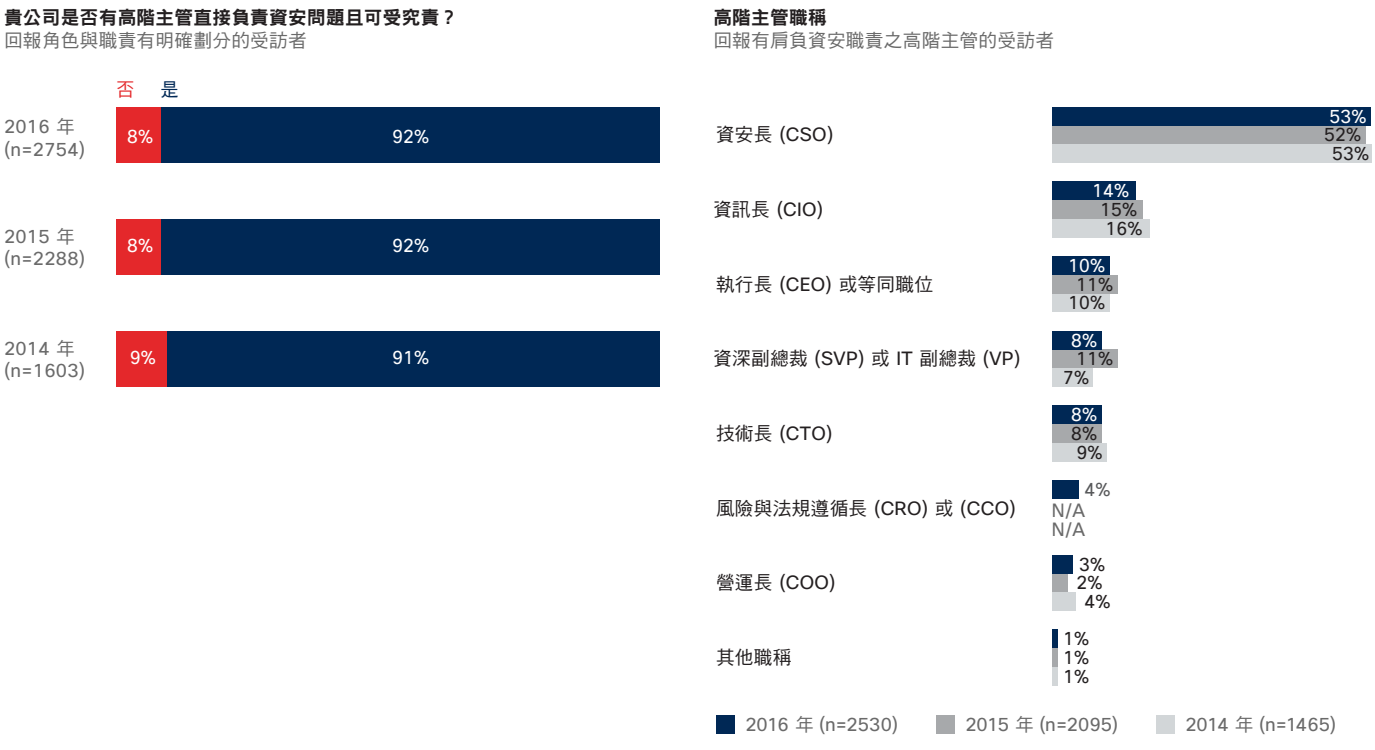
圖 88 外部部署私人雲端和協力廠商代管內部部署主機服務的增加程度

網路代管的位置	2014 (n=1727)	2015 (n=2417)	2016 (n=2887)
內部部署作為私有雲的一部分	50%	51%	50%
內部部署	54%	48%	46%
內部部署，但由外部第三方代管	23%	24%	27%
外部部署私有雲	18%	20%	25%
外部部署公有雲	8%	10%	9%

資料來源：思科 2017 年資安能力基準研究

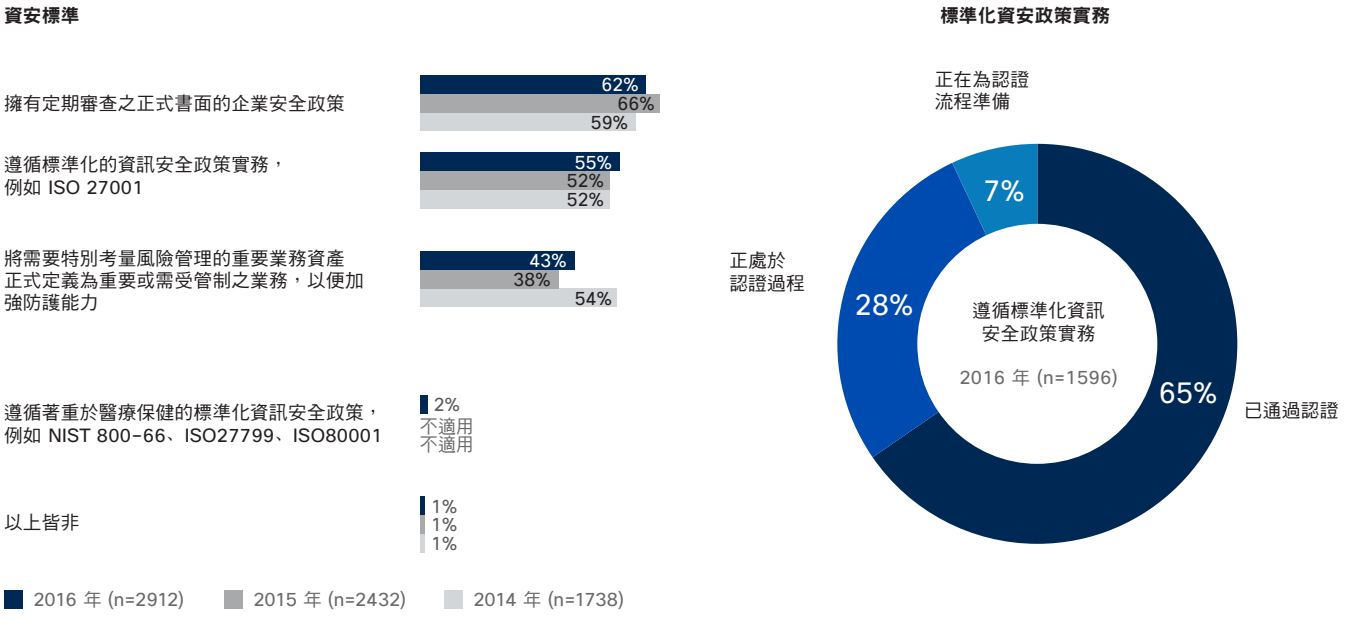
營運、原則、程序及功能

圖 89 聘雇資安主管的公司百分比



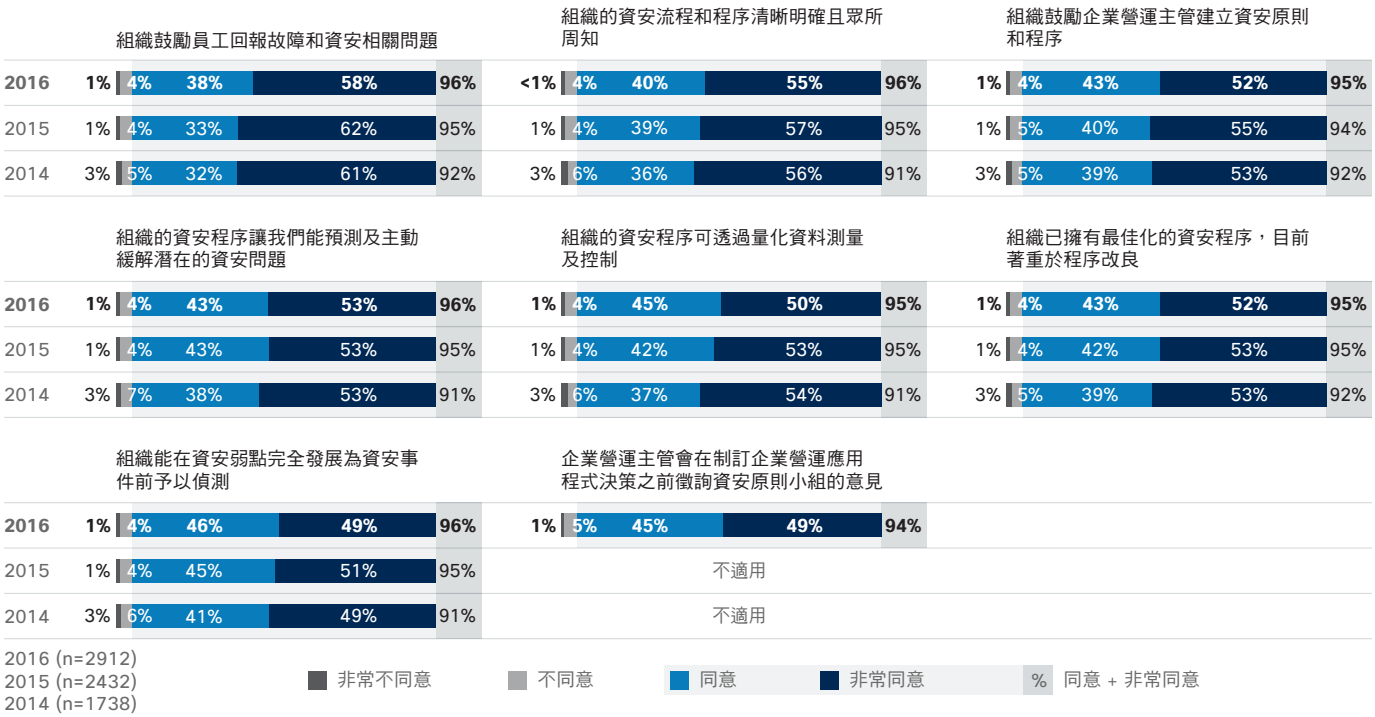
資料來源：思科 2017 年資安能力基準研究

圖 90 實施正式全公司資安策略及遵循標準化資安原則實務的公司百分比



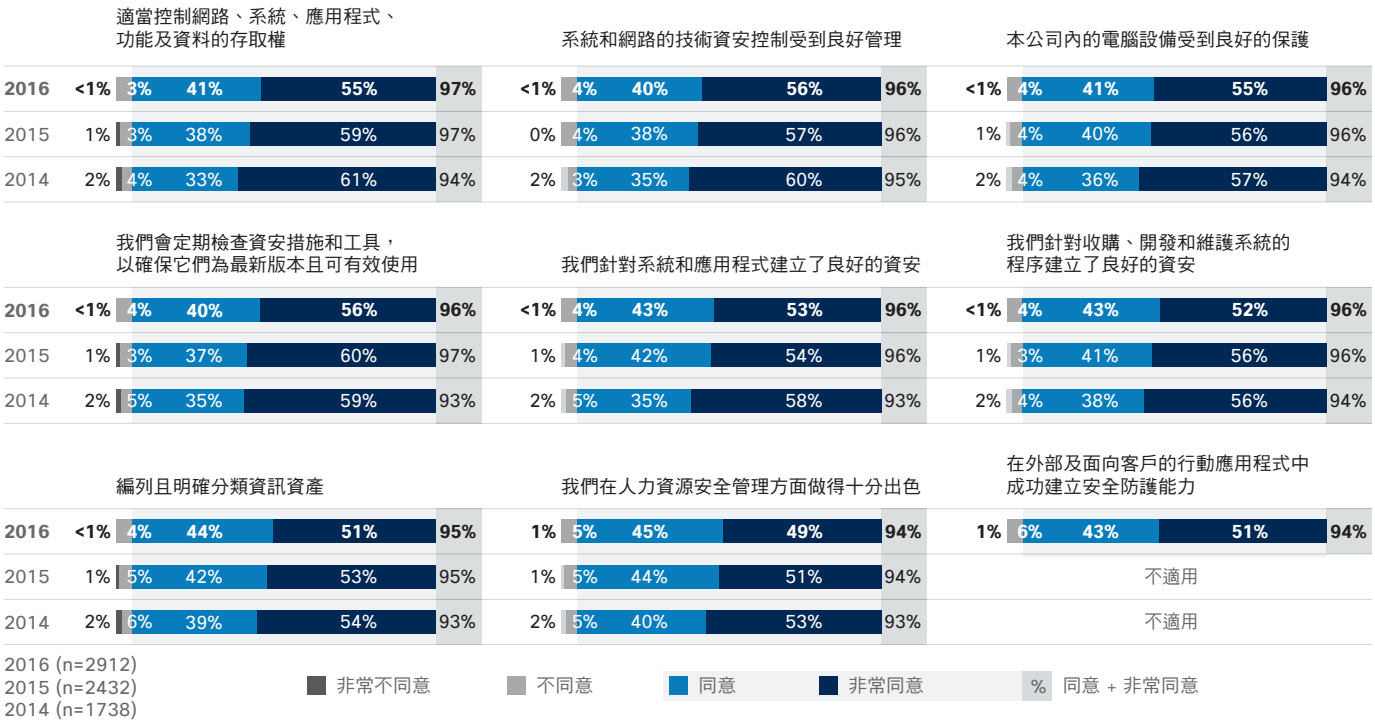
資料來源：思科 2017 年資安能力基準研究

圖 91 非常同意安全性程序聲明的受訪者百分比



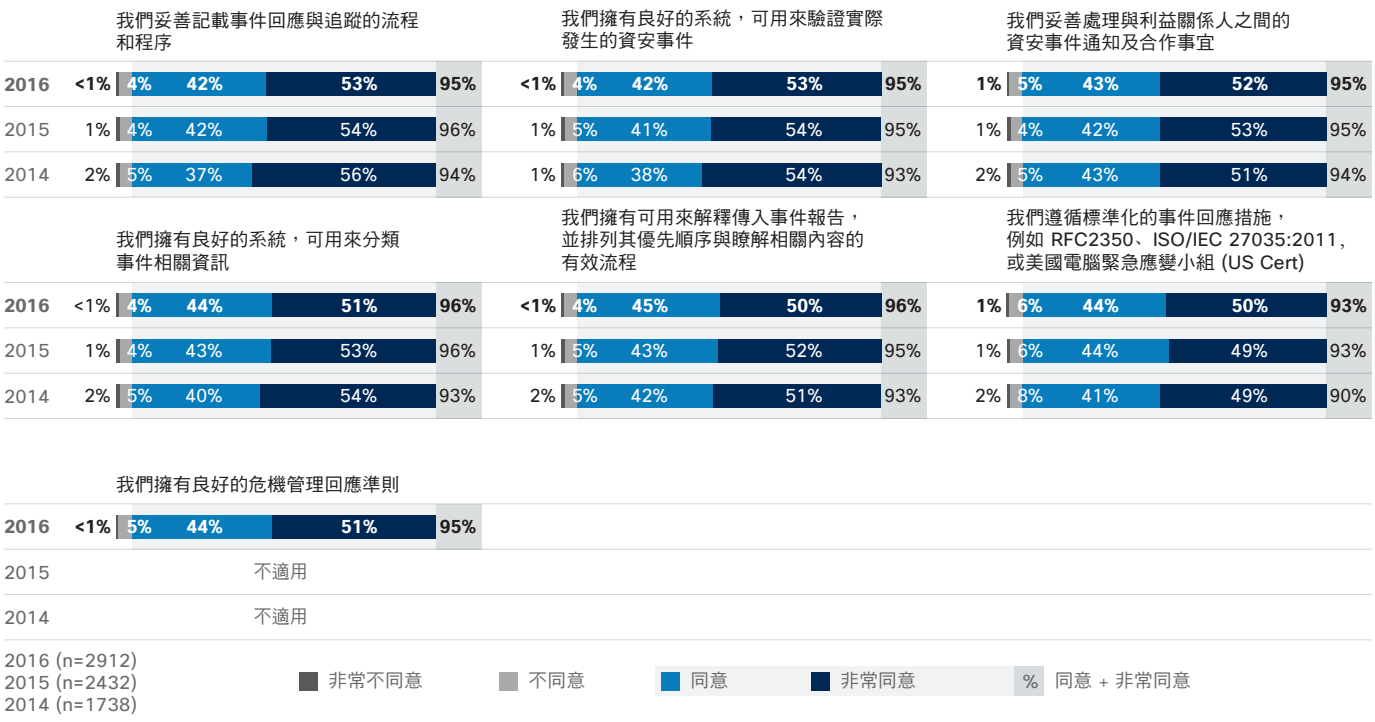
資料來源：思科 2017 年資安能力基準研究

圖 92 非常同意安全性程序聲明的受訪者百分比



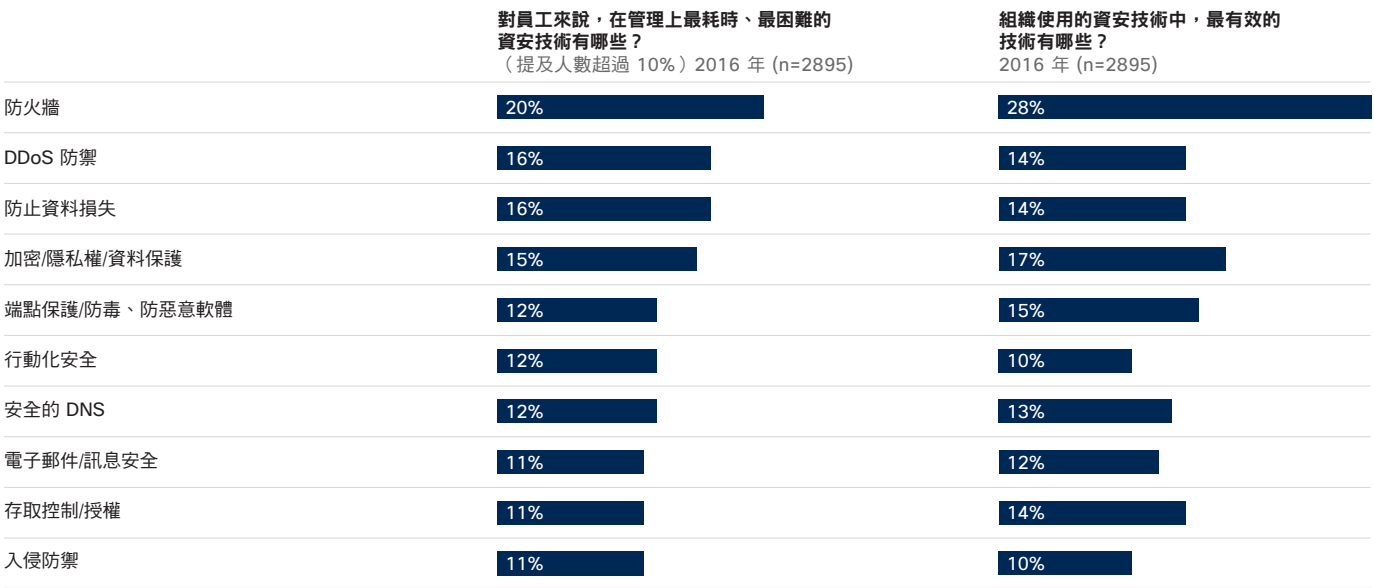
資料來源：思科 2017 年資安能力基準研究

圖 93 非常同意安全性控制聲明的受訪者百分比



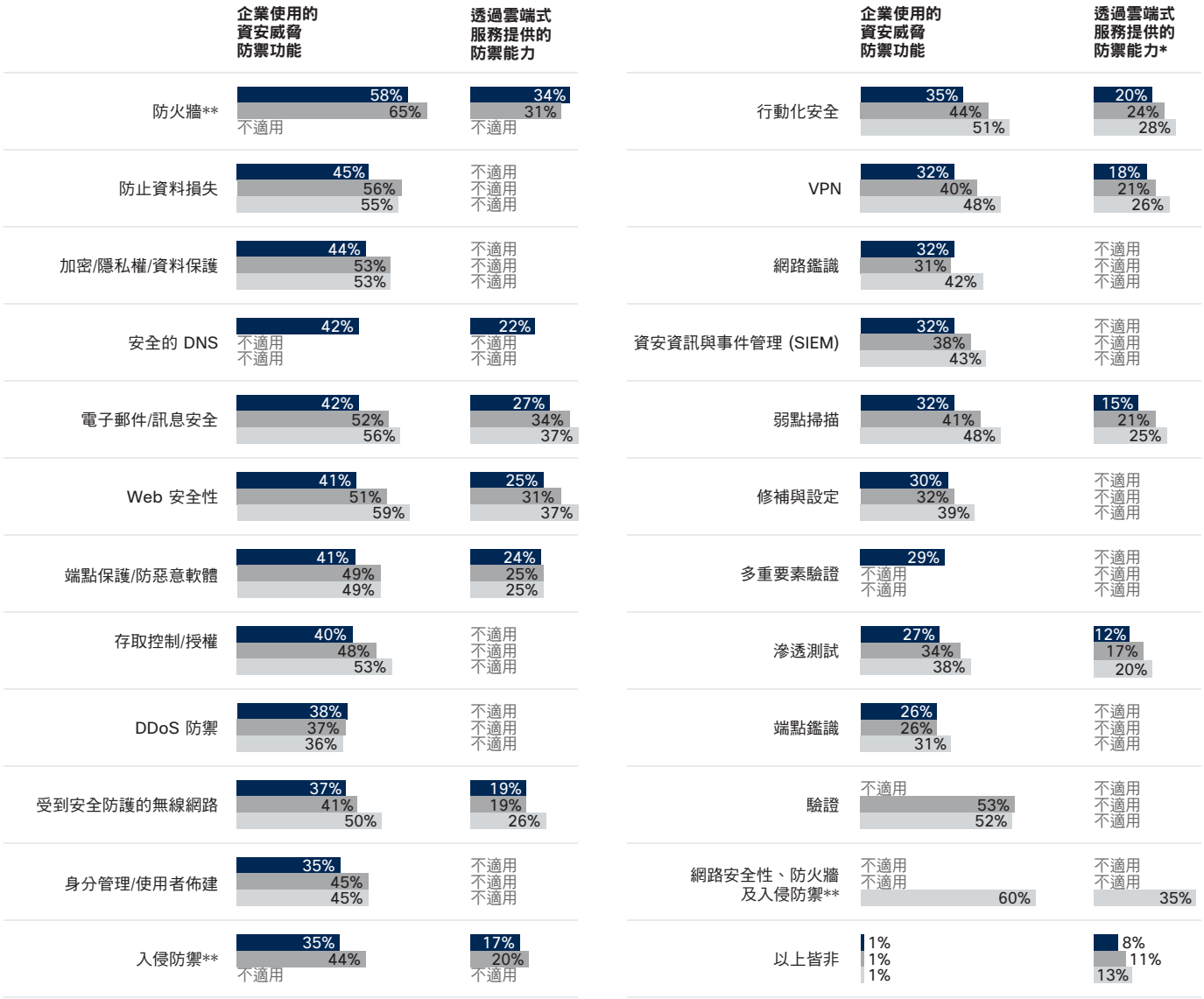
資料來源：思科 2017 年資安能力基準研究

圖 94 資安技術的管理和功效



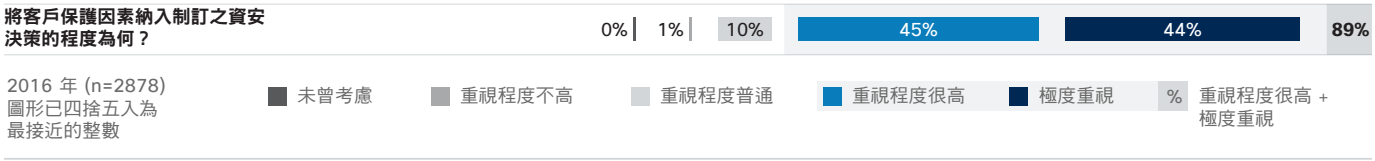
資料來源：思科 2017 年資安能力基準研究

圖 95 資安威脅防禦機制的逐年使用程度



資料來源：思科 2017 年資安能力基準研究

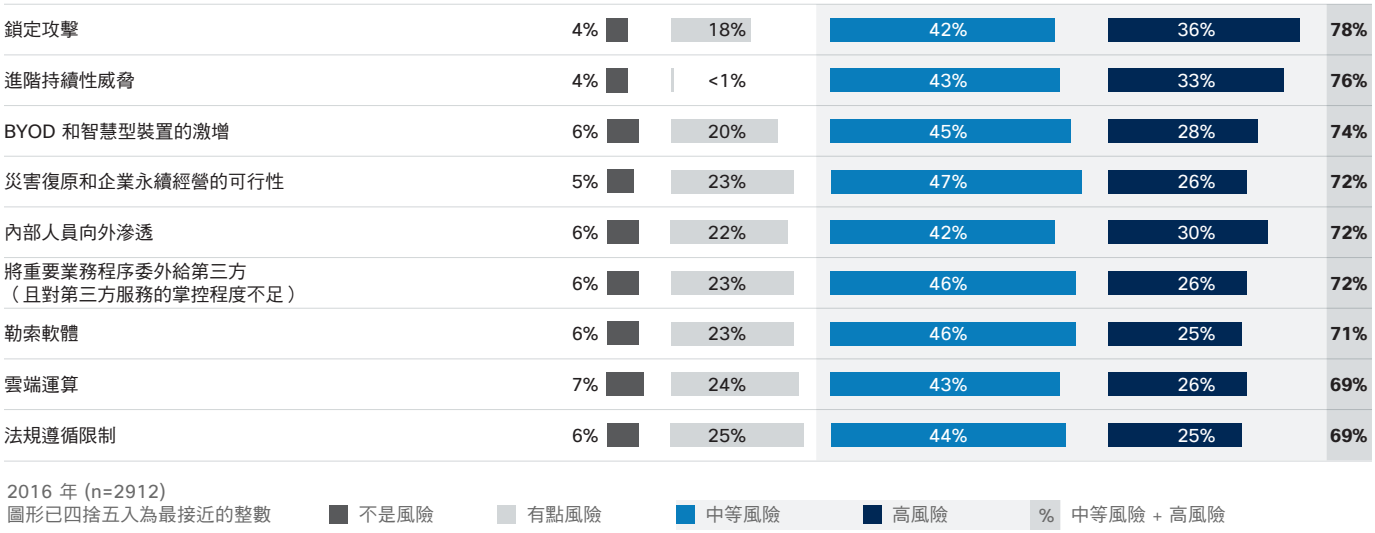
圖 96 將客戶保護因素納入制訂之資安決策的程度



資料來源：思科 2017 年資安能力基準研究

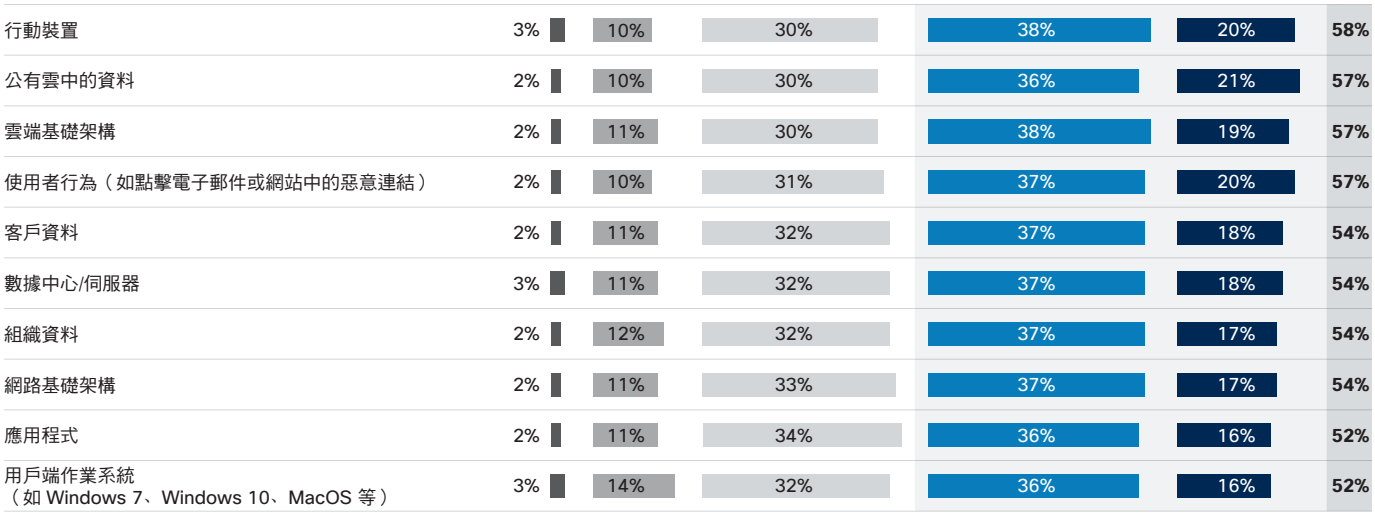
風險和弱點

圖 97 IT 資安人員之網路攻擊相關顧慮的最主要來源



資料來源：思科 2017 年資安能力基準研究

圖 98 資安專業人員之網路攻擊相關顧慮的最主要來源



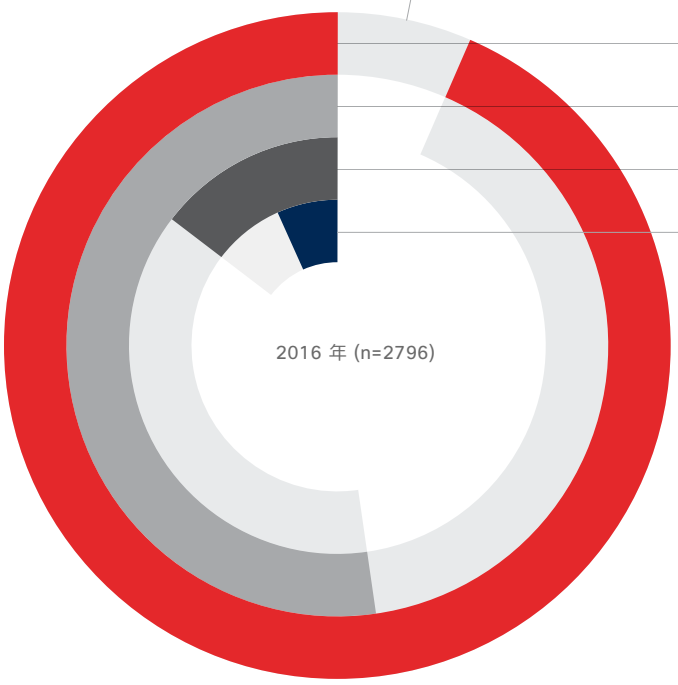
資料來源：思科 2017 年資安能力基準研究

圖 99 IT 團隊的勞力分佈

資料來源：思科 2017 年資安能力基準研究

事件回應

圖 100 經過調查或修復之資安警示的百分比



7% 未曾遭遇過資安警示

93% 曾遭遇過資安警示

56% 發現的警示均經過調查

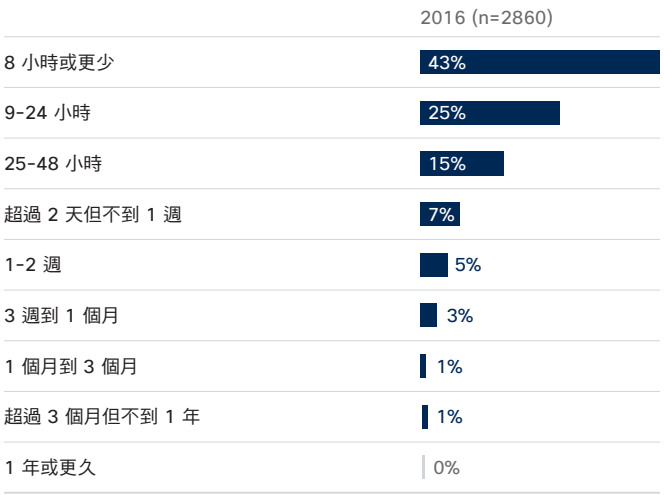
經過調查的警示中有 28% 是合法警示

46% 的合法警示經過修復

組織每天發現的警示平均數量	
不到 5K	50%
5K–10K	15%
10K–50K	11%
50K–100K	8%
100K–150K	6%
超過 150K	4%

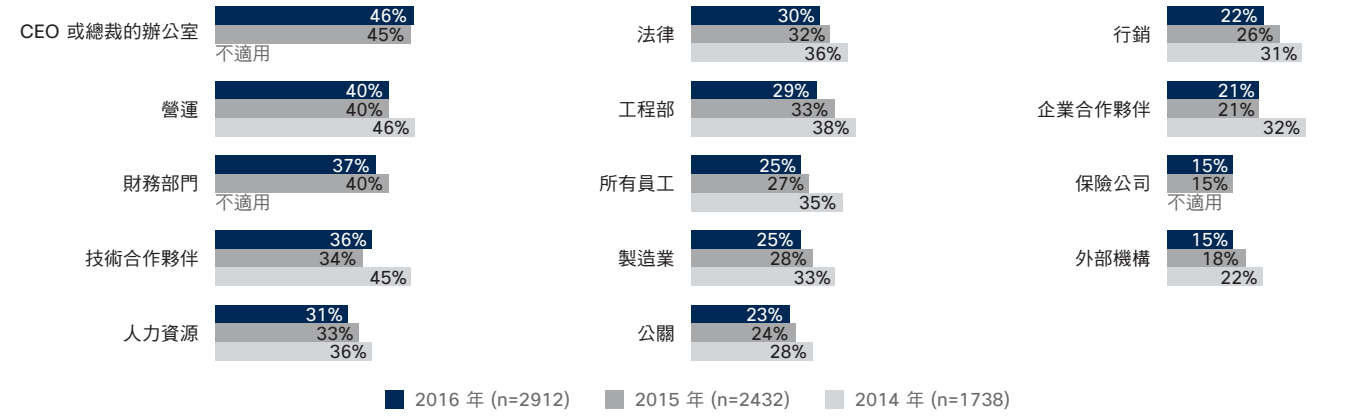
資料來源：思科 2017 年資安能力基準研究

圖 101 偵測資安漏洞的平均時間



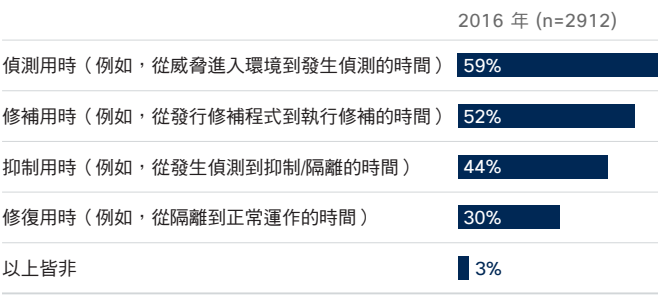
資料來源：思科 2017 年資安能力基準研究

圖 102 發生事件時的通知對象



資料來源：思科 2017 年資安能力基準研究

圖 103 組織用來評估資安績效的 KPI



資料來源：思科 2017 年資安能力基準研究

圖 104 逐年用來分析遭入侵之系統的程序

分析遭入侵之系統的程序	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
防火牆記錄	61%	57%	56%
系統記錄分析	59%	53%	50%
網路流量分析	53%	49%	49%
惡意軟體或檔案回復分析	55%	48%	47%
註冊分析	50%	47%	43%
完整的封包擷取分析	47%	38%	40%
IOC 偵測	38%	35%	38%
磁碟鑑識	40%	36%	36%
關聯的活動/記錄分析	42%	37%	35%
記憶體鑑識	41%	34%	34%
外部事件回應/分析團隊	37%	33%	34%
以上皆非	2%	1%	1%

資料來源：思科 2017 年資安能力基準研究

圖 105 逐年用來消除資安事件肇因的程序

可消除資安事件肇因的流程	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
隔離或移除惡意應用程式	58%	55%	52%
根本原因分析	55%	55%	51%
停止惡意軟體的通訊	53%	53%	48%
其他監控	52%	48%	48%
政策更新	51%	47%	45%
停止遭入侵之應用程式的通訊	48%	47%	43%
開發長期修正程式	47%	40%	41%
重新製作系統的映像以回復先前狀態	45%	41%	39%
以上皆非	2%	1%	1%

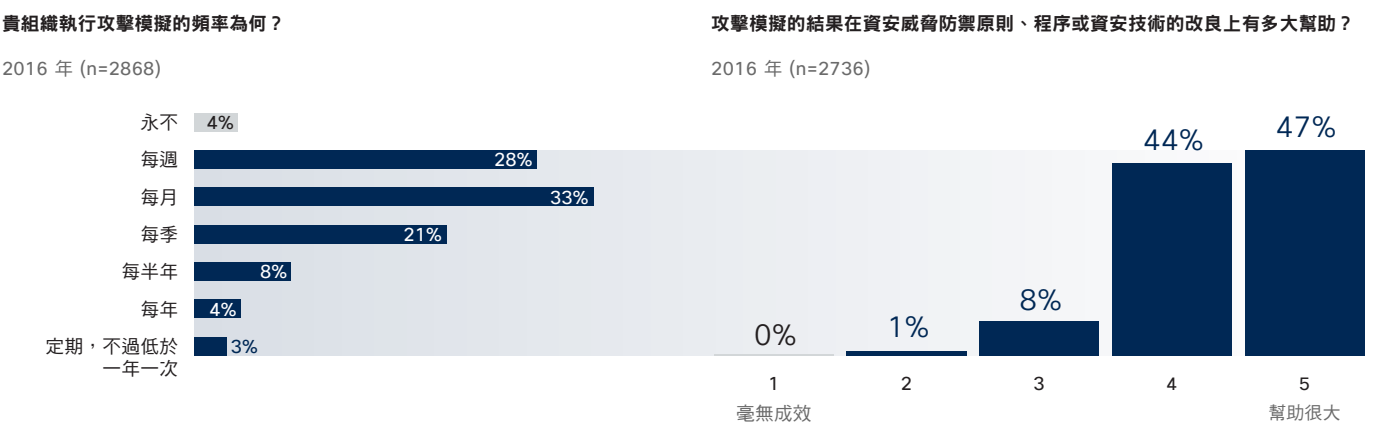
資料來源：思科 2017 年資安能力基準研究

圖 106 逐年用來還原受影響之系統的程序

還原受影響系統的流程	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
根據事件後已識別的弱點，執行其他或新的偵測和控制	60%	56%	56%
從事件前備份中還原	57%	59%	55%
修補和更新容易受到攻擊的應用程式	60%	55%	53%
還原差別（移除事件造成的變更）	56%	51%	50%
黃金影像還原	35%	35%	34%
以上皆非	2%	1%	1%

資料來源：思科 2017 年資安能力基準研究

圖 107 攻擊模擬：推動資安防禦改良措施的頻率和程度



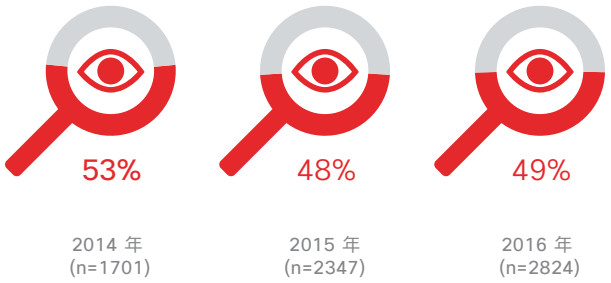
資料來源：思科 2017 年資安能力基準研究

圖 108 探究資安漏洞之來源的重要性

資料來源：思科 2017 年資安能力基準研究

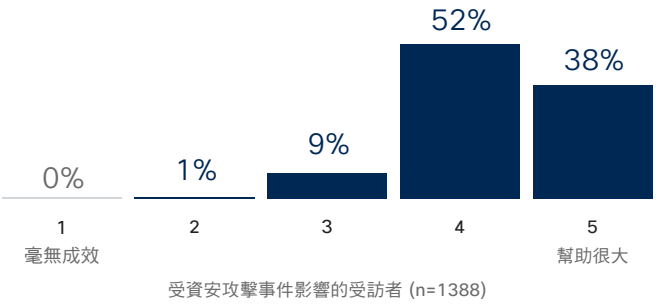
漏洞和影響

圖 109 遭遇公共漏洞的組織百分比



資料來源：思科 2017 年資安能力基準研究

圖 110 資安漏洞在資安威脅防禦原則、程序或技術的改良上有多大幫助？

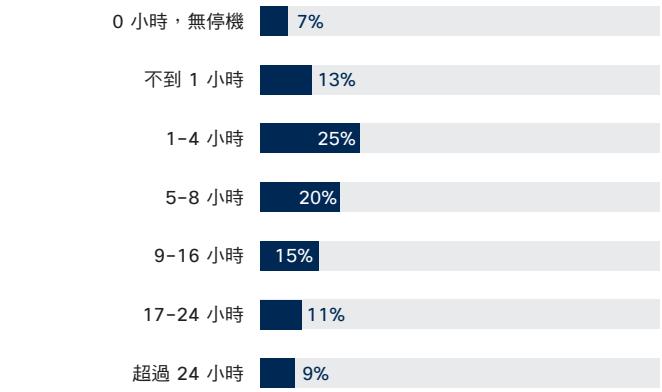


資料來源：思科 2017 年資安能力基準研究

圖 111 由資安漏洞引起之營運中斷的時間長度和程度

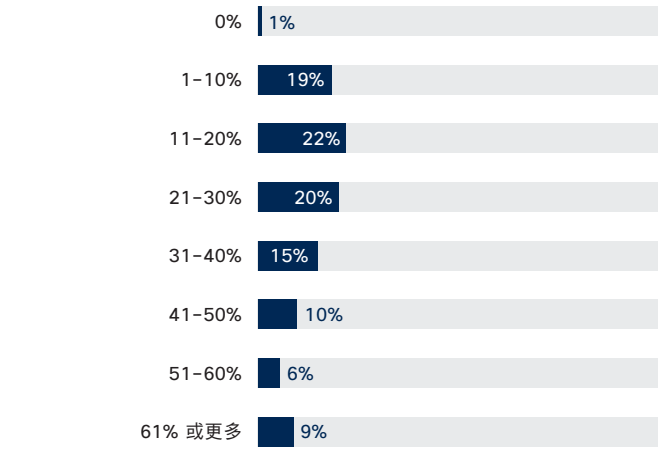
由攻擊事件所引起的系統停機時間

2016 (n=2665)



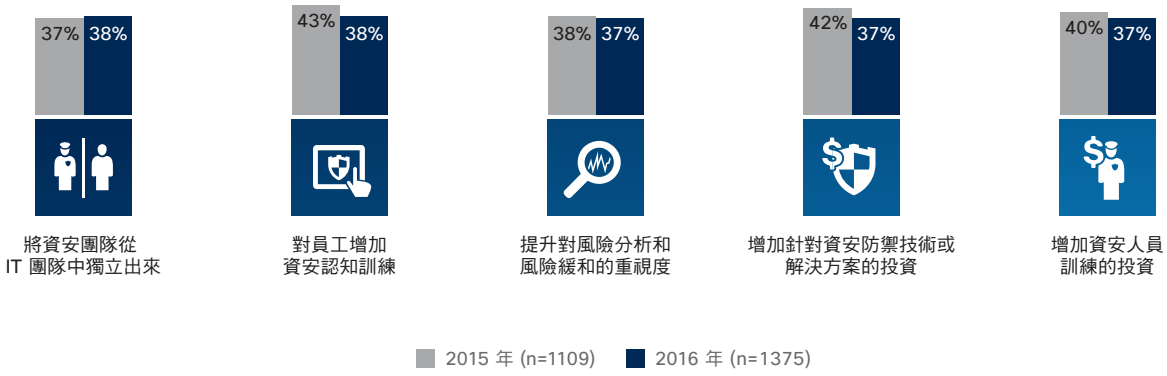
因攻擊事件而受影響的系統百分比

2016 (n=2463)



資料來源：思科 2017 年資安能力基準研究

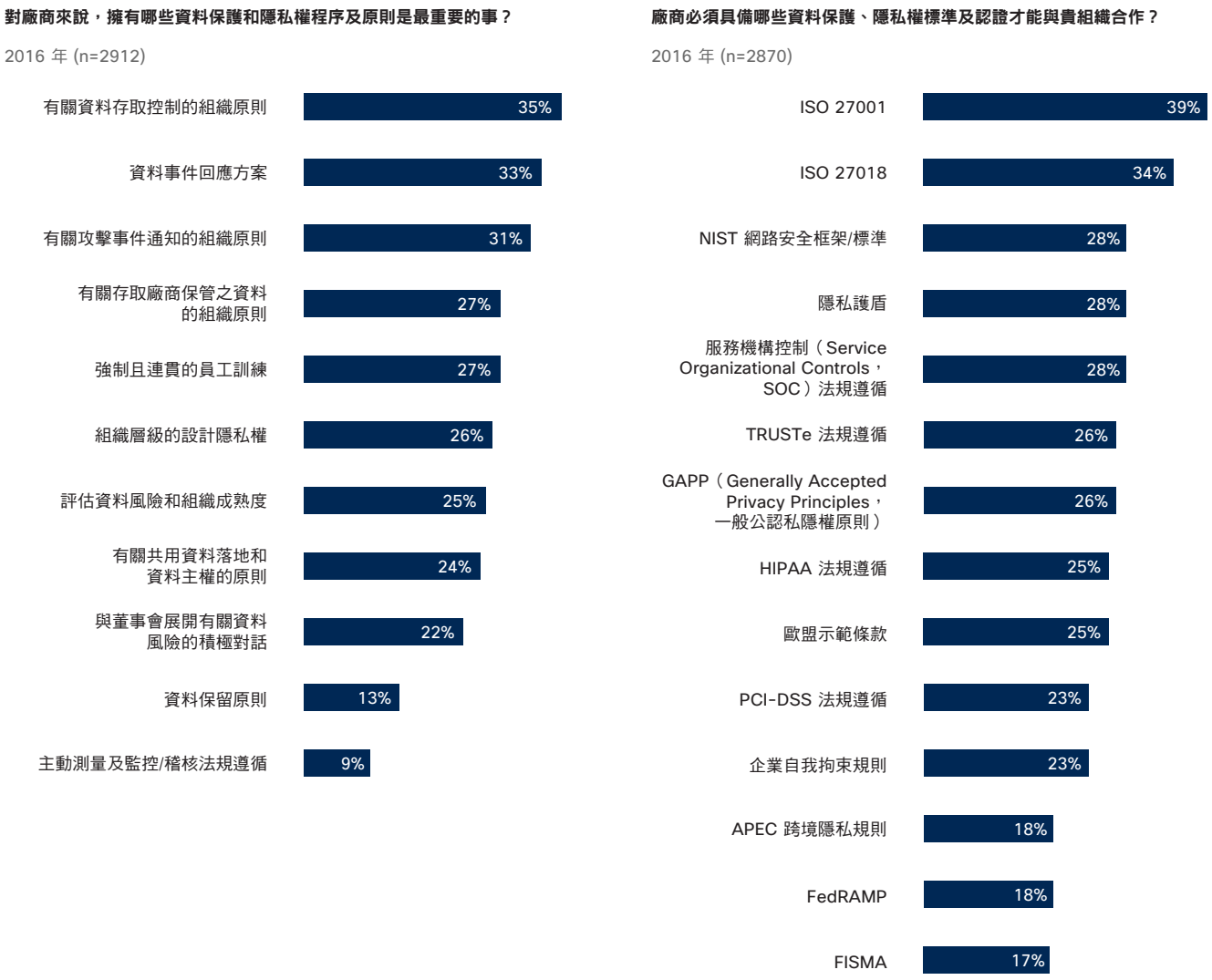
圖 112 為了預防公司出現資安漏洞所做的改良措施



資料來源：思科 2017 年資安能力基準研究

廠商選擇和期望

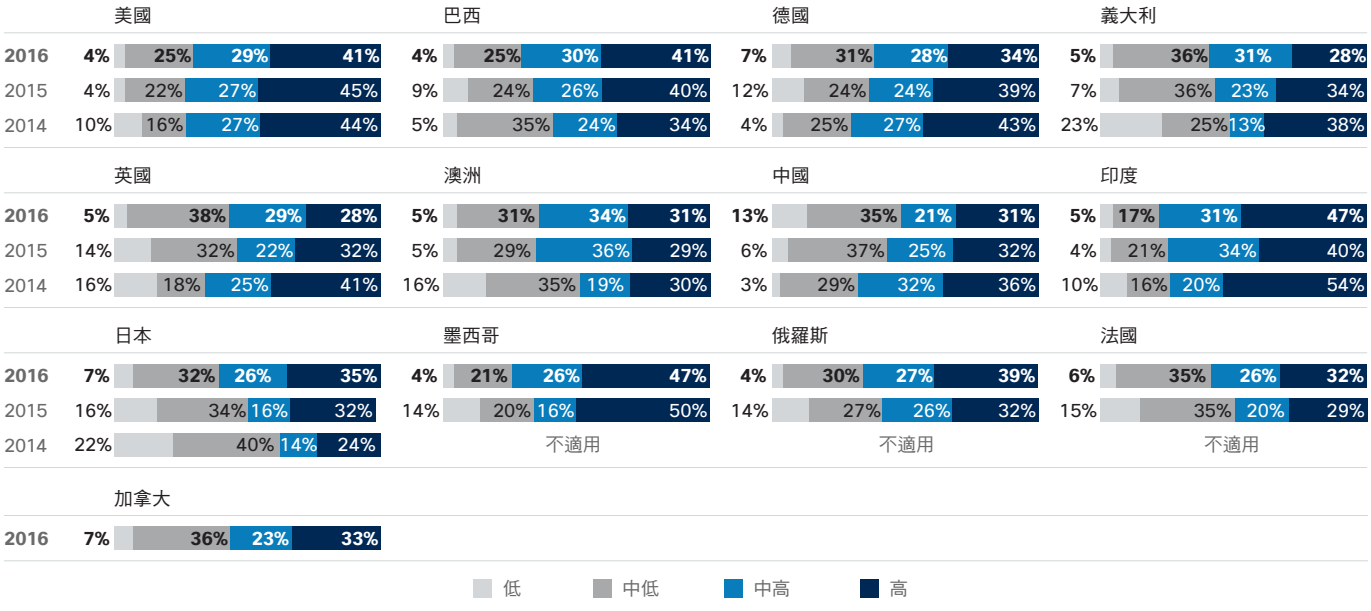
圖 113 資料保護和隱私權對廠商的重要性



資料來源：思科 2017 年資安能力基準研究

資安能力成熟模型

圖 114 依據國家排列的資安成熟度

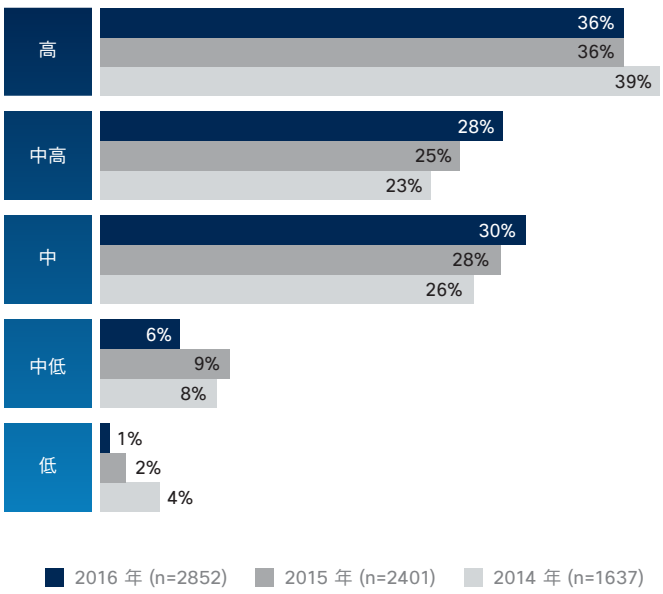


資料來源：思科 2017 年資安能力基準研究

圖 115 依安全性程序對組織進行成熟模型分級

資料來源：思科 2017 年資安能力基準研究

圖 116 成熟模型的區段大小

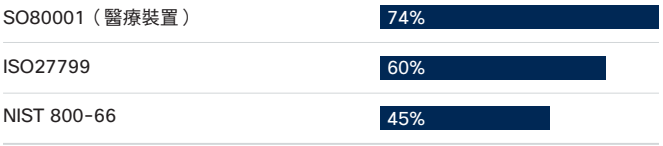


資料來源：思科 2017 年資安能力基準研究

產業特有

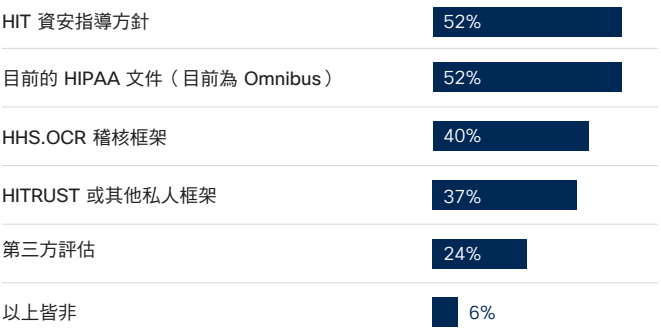
圖 117 已執行標準化資安原則的醫療保健企業百分比

已執行標準化資安原則
醫療保健企業遵循醫療保健特有的資訊安全原則實務（2016 年；n=65）



資料來源：思科 2017 年資安能力基準研究

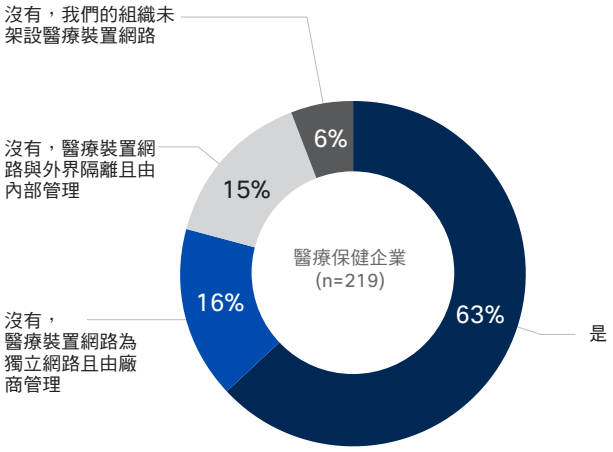
圖 118 醫療保健公司用來自我評量對 HIPAA 隱私權規則之遵循程度的資源



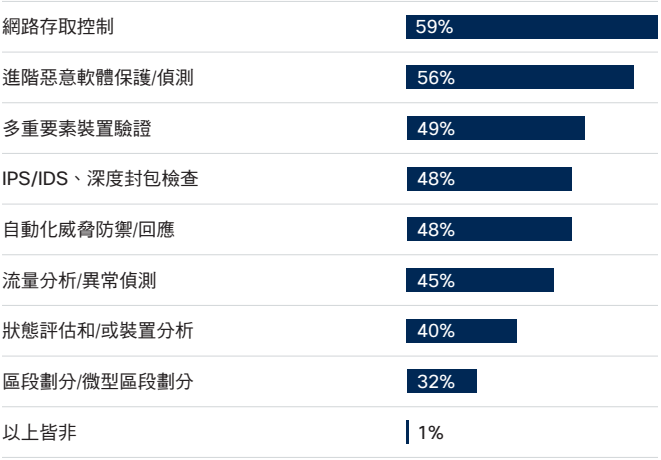
資料來源：思科 2017 年資安能力基準研究

圖 119 架設醫療裝置網路之醫療保健企業最常用的安全措施

貴組織是否擁有向主要醫院網路匯集的醫療裝置網路？



貴公司執行以下哪些安全措施（若有的話）來保護醫療裝置網路？
在組織中架設醫療裝置網路的公司 (n=207)



資料來源：思科 2017 年資安能力基準研究

圖 120 電信業的範例個人資料

貴組織目前主要從事哪項電信業子區段的業務？
電信業企業 (n=307)

通訊設備	47%
服務供應商（傳統）	33%
第四台/衛星電視營運商	11%
媒體/廣播	7%
機上盒供應商（Netflix、Hulu 等）	2%

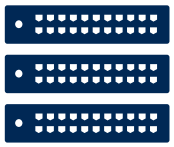
貴公司提供以下哪些服務給客戶？
電信業企業 (n=308)

提供給終端客戶的代管資安服務	71%
核心生產網路，如 IP（包括電視）、行動服務等。	60%
企業環境	59%
資料中心	57%

資料來源：思科 2017 年資安能力基準研究

圖 121 電信業的資安策略因素

資安策略和準則的相對優先順序
電信業企業 (n=308)



平均可用性百分比

34%

可用性：確保可靠的資料存取

平均機密性百分比

36%

機密性：確保唯有適當的對象才能存取資料

平均完整性百分比

31%

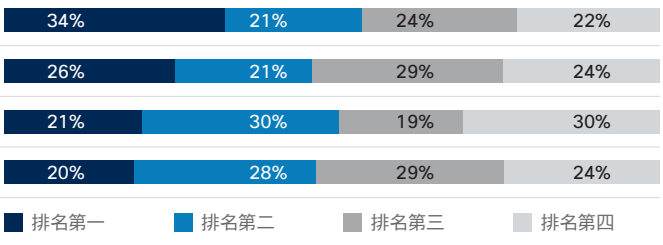
完整性：確保資料精確

資料來源：思科 2017 年資安能力基準研究

圖 122 電信業的資安優先要務

組織資安優先要務的排名

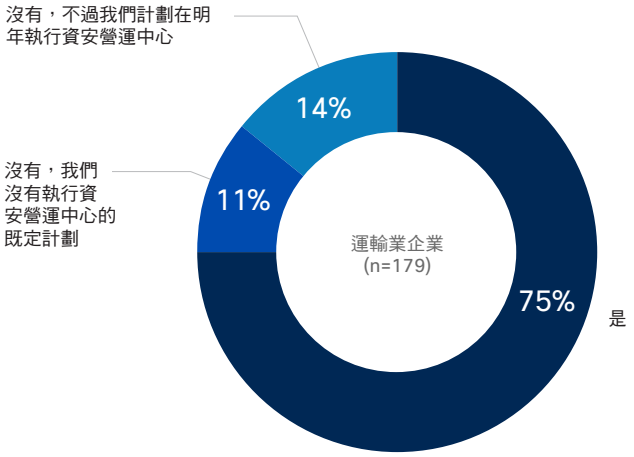
電信業企業 (n=308)



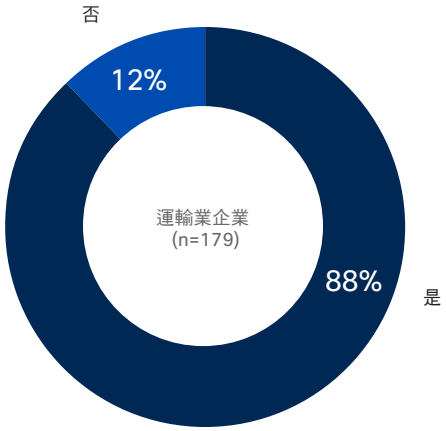
資料來源：思科 2017 年資安能力基準研究

圖 123 運輸業的範例個人資料

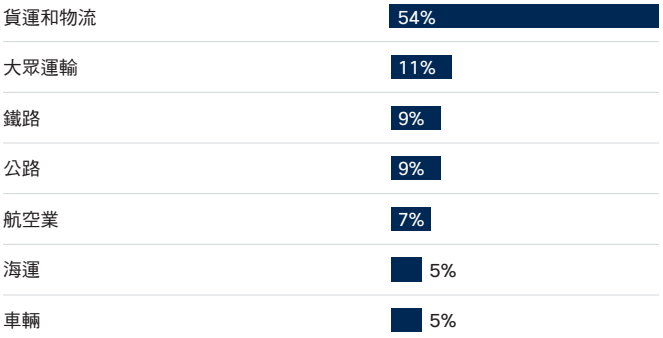
貴公司是否使用資安營運中心（Security Operations Center，SOC）？



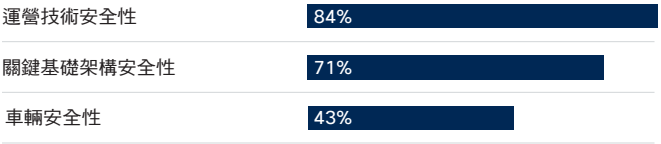
貴公司是否參與資安標準團體或產業組織？



貴組織目前主要從事哪項運輸業子區段的業務
運輸業企業 (n=180)



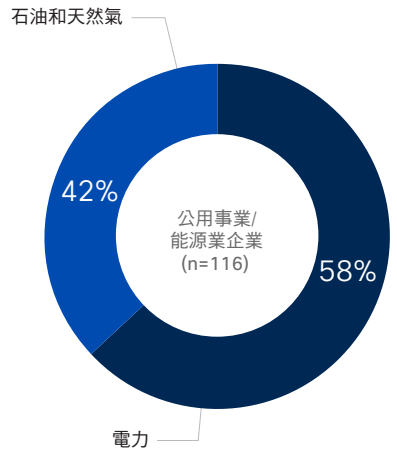
您負責以下哪些資安領域的事務？
運輸業企業 (n=180)



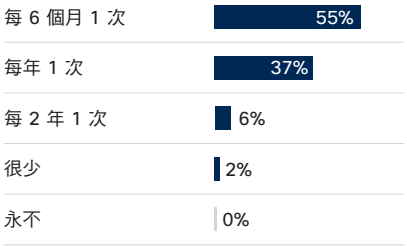
資料來源：思科 2017 年資安能力基準研究

圖 124 公用事業/能源業的範例個人檔案

貴組織目前主要從事哪項公用事業/能源業子區段的業務？

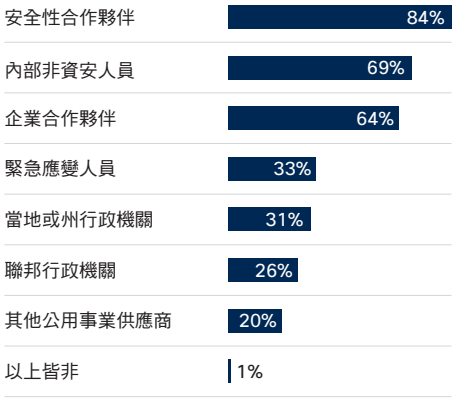


貴公司實施演習來測試公司對網路資安事件之回應計劃的頻率為何？



公用事業/能源業企業 (n=116)

貴公司實施以下哪些演習？參與的對象為何？

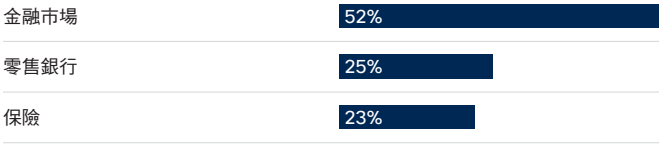


公用事業/能源業企業 (n=116)

資料來源：思科 2017 年資安能力基準研究

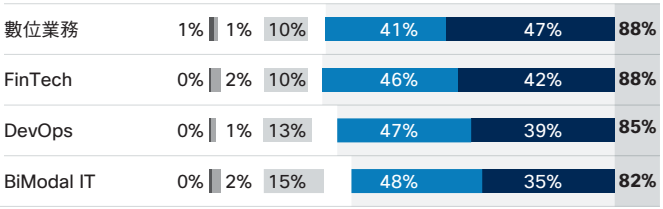
圖 125 金融服務業的範例個人檔案

貴組織目前主要從事哪項金融服務業子區段的業務？



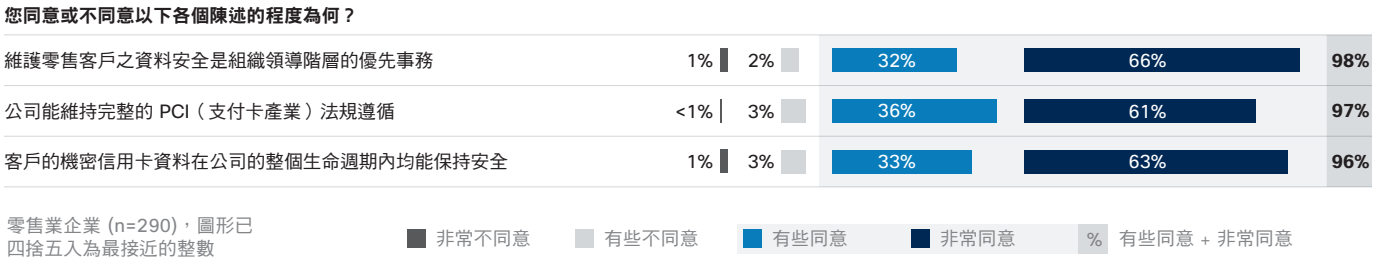
金融服務業企業 (n=509)
圖形已四捨五入為最接近的整數

您認為以下趨勢對資安的影響程度為何



資料來源：思科 2017 年資安能力基準研究

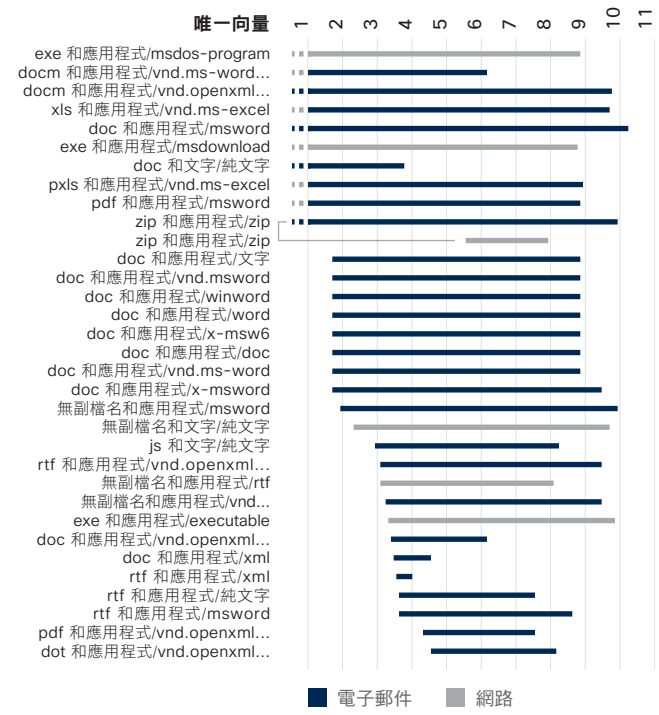
圖 126 零售業的資料安全性



資料來源：思科 2017 年資安能力基準研究

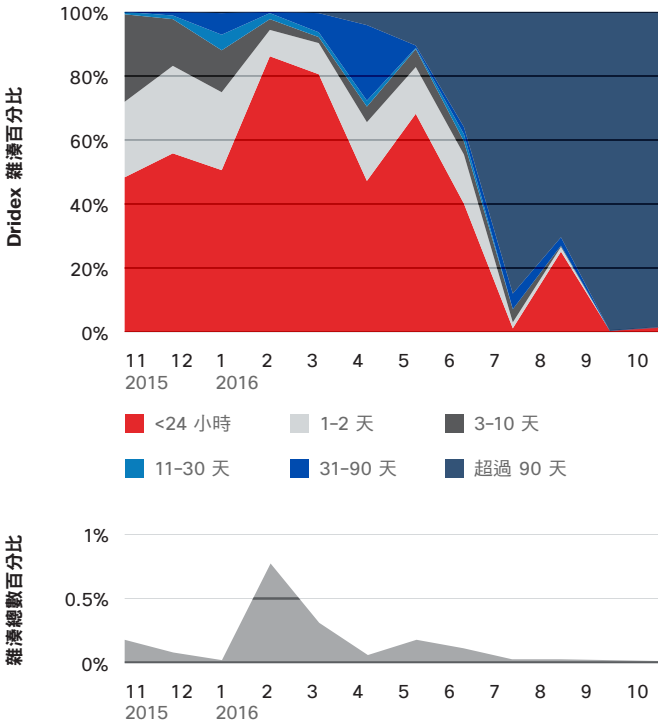
惡意軟體系列

圖 127 Dridex 的檔案副檔名和 MIME 組合（網路和電子郵件向量）



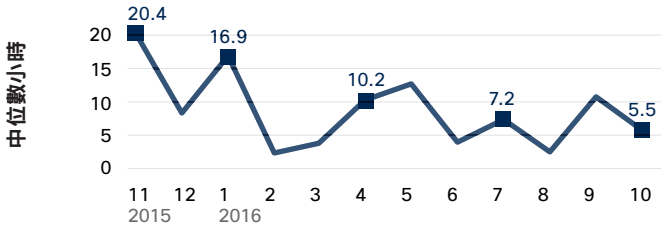
資料來源：思科資安研究部門

圖 128 Dridex 惡意軟體系列的雜湊存留時間和每個月觀察到之雜湊總數量百分比



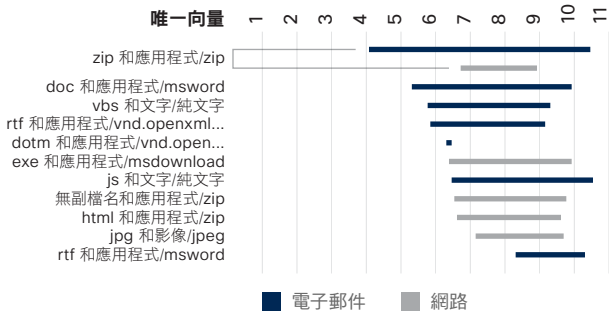
資料來源：思科資安研究部門

圖 129 Dridex 惡意軟體系列的 TTD



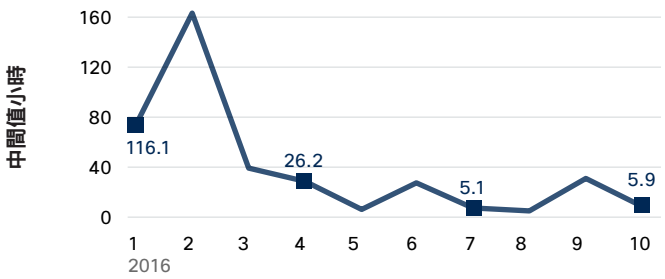
資料來源：思科資安研究部門

圖 130 威脅系列的檔案副檔名和 MIME 組合，以及可追溯到和包含 Cerber 承載的指標（網路和電子郵件向量）



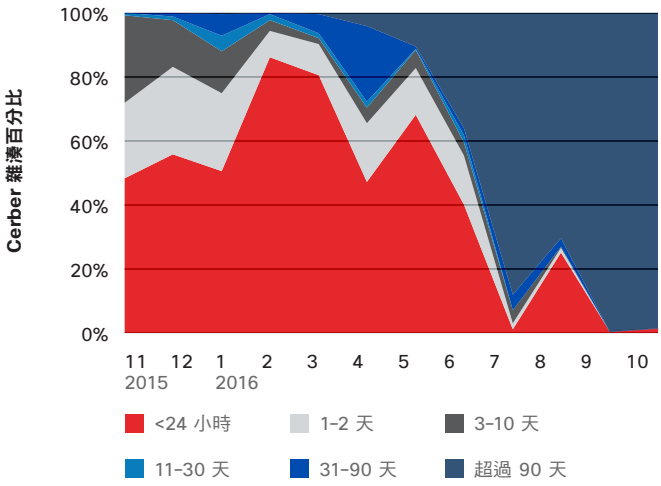
資料來源：思科資安研究部門

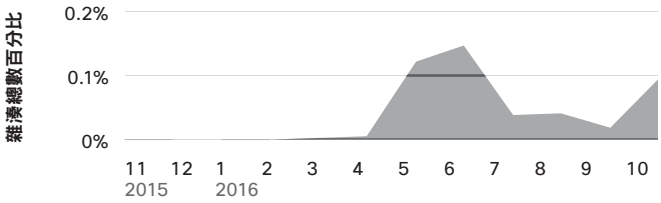
圖 131 Cerber 惡意軟體系列的 TTD



資料來源：思科資安研究部門

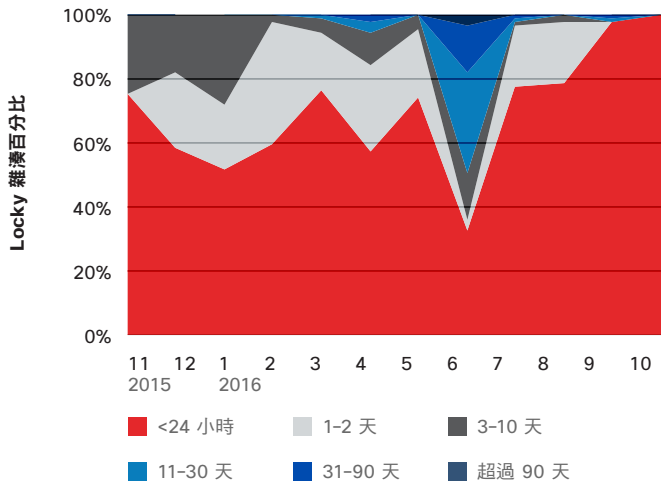
圖 132 Cerber 惡意軟體系列的雜湊存留時間和每個月觀察到之雜湊總數量百分比





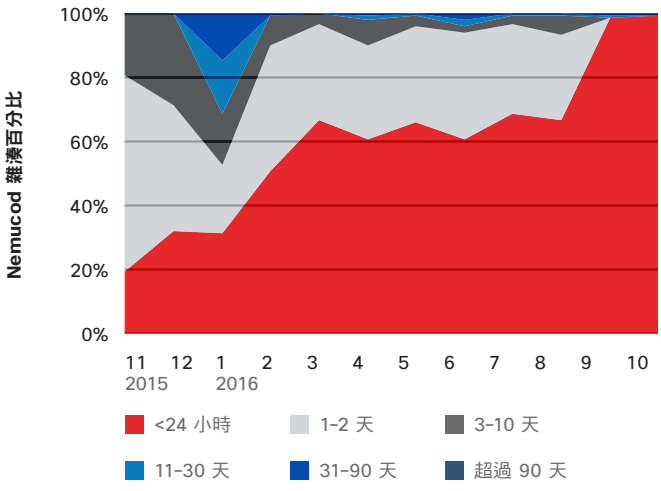
資料來源：思科資安研究部門

圖 133 Locky 惡意軟體系列每個月的雜湊存留時間



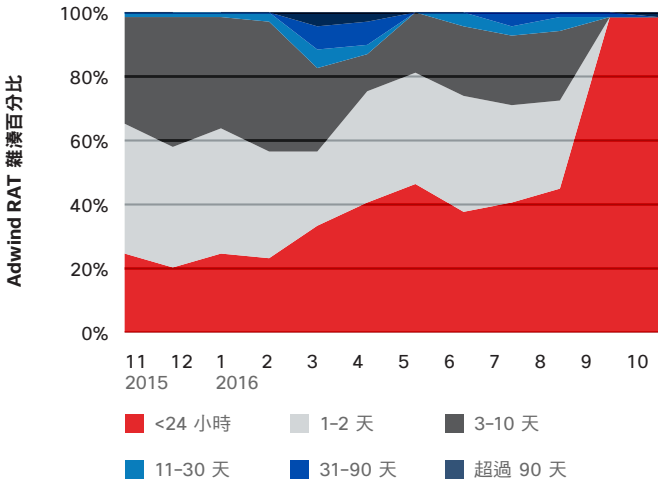
資料來源：思科資安研究部門

圖 134 Nemucod 惡意軟體系列每個月的雜湊存留時間



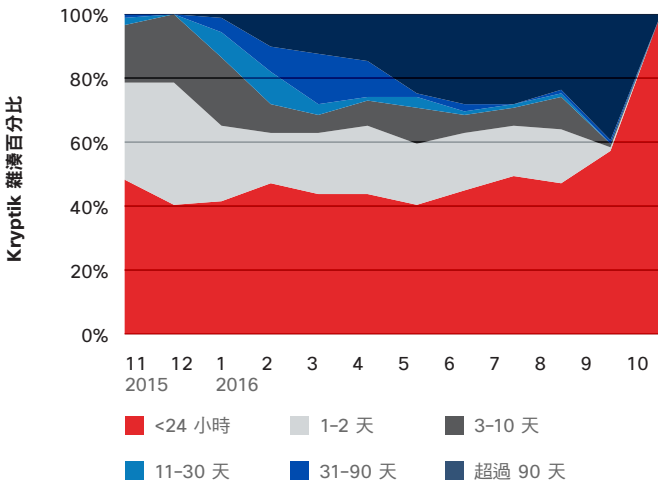
資料來源：思科資安研究部門

圖 135 Adwind RAT 惡意軟體系列每個月的雜湊存留時間



資料來源：思科資安研究部門

圖 136 Kryptik 惡意軟體系列每個月的雜湊存留時間



資料來源：思科資安研究部門

下載圖表

本報告的所有的圖表可在
www.cisco.com/go/acr2017graphics 下載。

更新和修正

如需參閱本報告的更新和修正內容，請造訪
www.cisco.com/go/acr2017errata

美洲總部
Cisco Systems, Inc.
San Jose, CA

亞太總部
Cisco Systems (USA) Pte. Ltd.
新加坡

歐洲總部
Cisco Systems International BV Amsterdam,
荷蘭

思科在全球各地設有超過 200 個分公司。各分公司地址、電話及傳真號碼皆列於思科網站上，網址為：www.cisco.com/go/offices。

2017 年 1 月出版