安全威脅控制與封鎖：回應不斷變遷之安全威脅的新策略

引言

網路安全威脅有可能大幅阻礙生產力，中斷商務與營運，造成資料遺失—而進一步導致財務損失與背負潛在的法律責任。駭客仍持續開發新的技術，獲取資料以從中牟利。

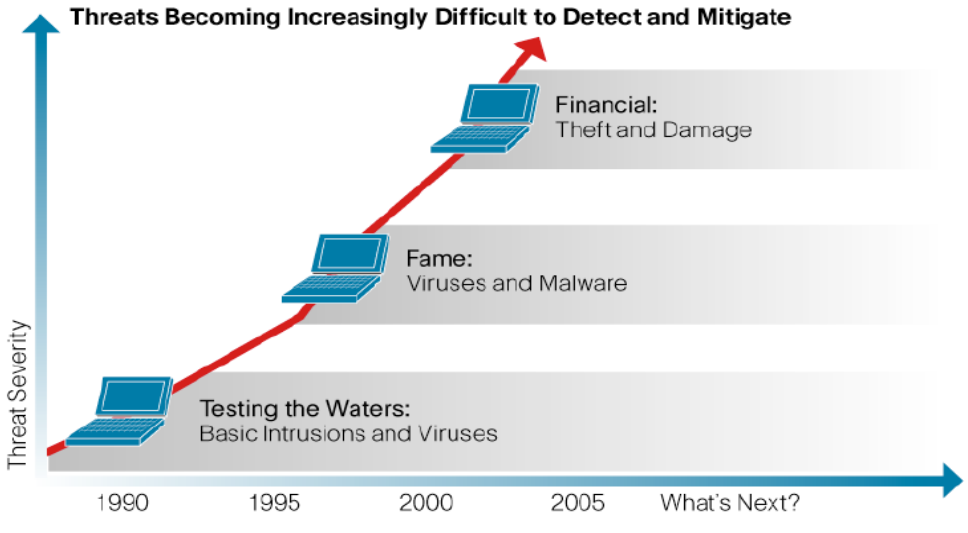
必須要用更主動式的網管安全策略，才能因應安全威脅的演進與複雜度，以確保商業營運的連續性，提供整體網路基礎架構的能見度與保護以免於威脅，並簡化平常每日的網路管理。完整的安全基礎架構—網路、系統、與管理—必須協同合作，以主動防禦多樣化的網路威脅，並降低回應與解決安全事件的時間。思科的安全威脅控制解決方案具備全面與主動的網路防禦機制，精簡安全政策與系統管理，以維持營運連續性。

變遷中的安全威脅

曾經一度，名氣是駭客利用系統與網路弱點的主要目的。今日，愈來愈多破壞系統的行為，是為了從中牟利。動機的改變導致使用方法也隨之不同，也讓偵測與解決系統攻擊行為愈來愈困難。(見圖一)

駭客調整的速度，比軟體與作業系統供應商推出修補程式與臨時解決方法的速度還要快。這些攻擊經常都針對特定的系統弱點，而網路安全機制無法辨識與阻止。除了大規模的蠕蟲與病毒爆發之外，IT企業還需要保護網路免於那些特別設計，以避開偵測並躲過傳統防禦系統的安全威脅發生。

Figure 1. The Changing Threat Landscape



表一 變遷中的網路安全威脅圖像

表一 威脅愈來愈難偵測與化解

爲了牟利：竊取資訊與破壞系統

爲了名氣：病毒與惡意軟體

威脅嚴重度

只是試水溫：基本的網路入侵與病毒

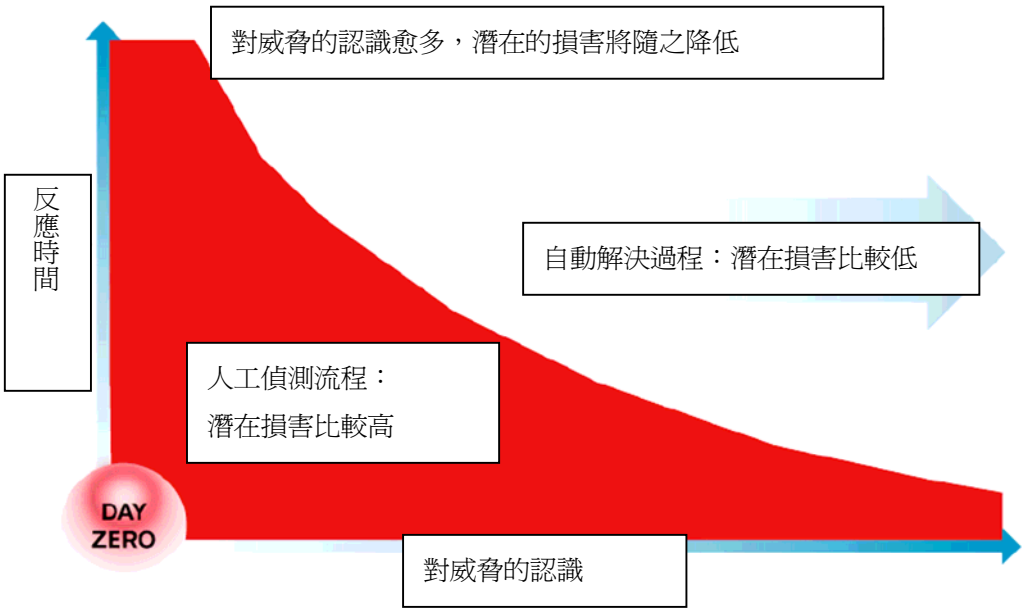
自

動調適型政策與技術，以打擊新型威脅

新型威脅(經常被稱為「day-zero」威脅)更難察覺與解決，因為缺乏對這樣攻擊型態的了解而無法預防。不幸的是，許多網管部門都缺少流程或工具，可以自發、主動的預防攻擊、入侵、或其他對系統或是應用的惡意行為。除此之外，每日系統管理工作的負荷、使用者來電、維修、稽核準備、與其他許多細項工作，經常阻礙企業專注防堵那些較難偵測到的安全威脅。

圖二 智慧型安全解決方案的好處

Figure 2. Benefits of an Intelligent Security Solution



由於因財務動機而啟動的系統攻擊愈來愈多，網管部門需要對整體網路基礎架構有全面的能見度，以俾將回應安全事件的時間降至最低。企業必須有工具可以偵測違反安全政策、利用系統弱點、異常活動等狀況，以俾判定可疑與有害的網路流量。

360 度安全威脅能見度與保護

要打擊新型以及定義清楚的安全威脅，就必須對系統與網路基礎架構有更高、更深與更廣的能見度。要是能夠偵測到網路基礎架構中違反安全政策、剝削系統弱點、異常活動等狀況，企業可以更快速的確認出安全威脅。

簡化的安全威脅控制機制

網管部門持續擴增工具以打擊安全威脅，通常會導致有更多的工具套件：更多系統、更多流程、更多警報。管理異質性網路的安全政策，將可以確保對新型網路漏洞的控制。將安全情報系統與安全政策管理系統緊密結合有其必要性，將導入新安全政策的時間減至最低，以俾因應立即的安全威脅。

商業營運的連貫性

駭客持續發掘愈來愈多的網路弱點。因此，企業需要一個可自動調適的安全威脅預防策略。主動性安全威脅防禦不僅需要深層防護，還需要一個橫跨網路基礎架構各層次與各種元件的策略。終端主機、網路與管理系統必須協同合作，才能在安全事件發生時更快反應，並提供更佳的安全防護層級。

各種安全威脅的面向

不論是「day-zero」或是定義清楚的安全威脅，都有許多不同進入網路的方式，一個全面性的安全威脅控制政策與系統管理，都需要將這些納入考量。以下是威脅手法的簡介，以及當你持續完善安全威脅控制基礎架構時，所需要考量的事項：

保護被信任之使用者免於網路安全威脅

制止被信任之使用者與電腦將所安全威脅帶入網路，並在網路上執行、散播，對於使用者與 IT 的生產力，都會有很正面的影響。在很多狀況中，自動化的流程可以確保最高程度的防護，讓網路免於已知的攻擊，例如病毒。在處理蠕蟲與間諜軟體時，必須在它們對企業造成危害前，就先建置主動性防護機制以俾察覺並進而解決這些安全威脅。

安全威脅有三種進入網路的主要方式：業務通訊、系統感染、與內部傳染。

業務通訊

電子郵件、網站、檔案傳輸、即時通訊、與其他商務與個人通訊的方式，都可能將許多安全威脅帶給毫無戒心的使用者。由於許多人認為這些溝通方式完全安全，他們不會採取額外措施保護自己。在許多狀況中，安全威脅只是「煩人的事」，用標準防毒軟體來處理而已。然而，間諜軟體與資料外洩卻較難被查覺與監控，因此經常成為用來滲透毫無戒心使用者的方法。企業需要有全面性的作法，用最有效率的方式來反擊已知的安全威脅，也要有一個針對新型威脅有良好能見度的流程。能夠一開始就預防安全威脅通過閘道器進入網路，例如間諜軟體、病毒、垃圾郵件等，網管人員可以減輕所有終端主機的掃描負擔，以及掃描導致的效能影響。

系統感染

無論是線上或離線，行動與桌上型電腦都可能從不同來源被感染，並將這些感染帶入它們所使的企業網路。當一個行動電腦利用公共 Wi-Fi 存取點連上網路，然後連線回到辦公室或

是其他公司遠端據店，或者連上虛擬私有網路(VPN)時，上述情形就可能發生。行動電腦經常也是行竊的標的物，這也是另外一種它們會被惡意程式感染到的方式。這些電腦都面臨風險，因為它們經常被未被授權的使用者而使用，例如家庭成員。

確保這些終端主機的使用符合公司安全政策，並具備可接受的安全防護，乃是十分重要的事，因為這可以確保新的安全威脅無法利用被信任的使用者與設備，進入企業網路。在一個系統連上網路之前，就先確定該終端主機的安全狀態，可以讓網管人員用最不影響現有網路系統運作的方式，廣泛導入控制機制，並大幅降低安全威脅侵入的可能性。

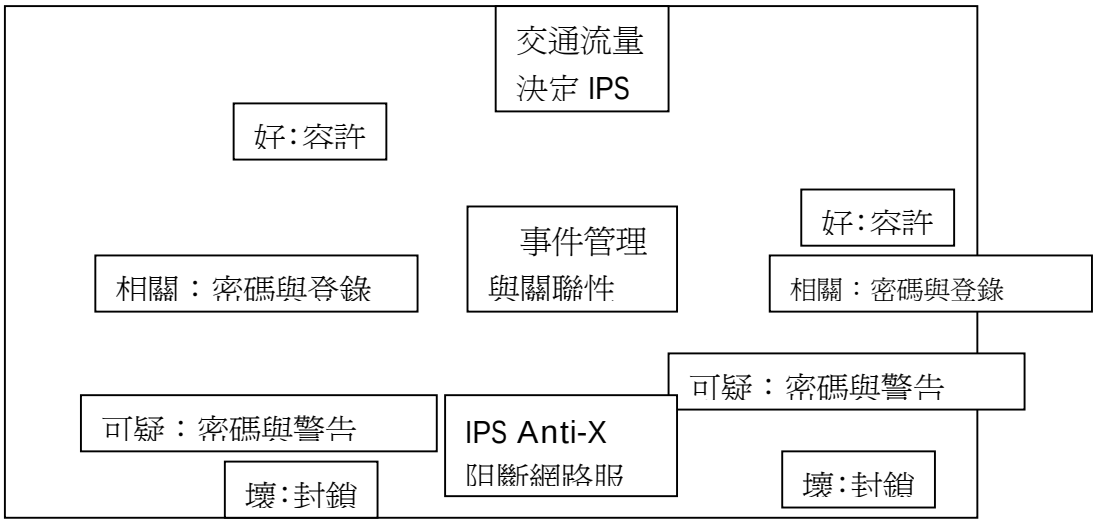
內部傳染

儘管用最大努力預防內部系統被感染，許多惡毒軟體還是有辦法躲開安全控管，並試圖啟動自己或將自己複製傳染其他受信任的系統。內部傳染經常比從網外滲透進來容易得多。透過對在終端主機上之異常行為與不必要軟體安裝的控制，可以預防安全威脅的感染與傳播。在此同時，透過有效管理稽核終端主機的系統狀態，例如記憶體與網路流量，可以預防「day-zero」安全威脅的發生。

保護伺服器免於攻擊與侵入

重要的資訊資產，例如人資記錄、財務資料、使用者資料庫、與幾乎所有電子化、數位化的商業資訊，都必須依風險等級分類，並依據企業制定的安全政策來保護。新的安全威脅已經出現，讓偵查與解決安全威脅侵入愈來愈困難。已經有工具與政策可以在網路漏洞被利用入侵前，就主動偵測潛在的安全威脅，新的安全機制具備更廣的能見度並改善偵測與化解威脅的功能，。這些新的工具與安全政策可以協助將風險降到最低，並縮短攻擊或侵入發生時的回應時間。圖三說明這些機制使用的某些流程，來確認可以允許那些類型的安全流量進入網路。

圖三　事件關聯性與降低資訊超載



事件關聯性與降低訊息超載

不論是在規模多大的安全事件發生時，安全系統、網路與設備主機經常產生大量的訊息。人工處理這些訊息可能會讓 IT 小組不勝負荷，讓標準工具變得沒效率，幾乎不可能即時發

現真正的安全威脅。想要將安全基礎架構的功效最大化，可以透過觀察安全威脅的模式，將這些事件進行風險等級歸類並做關聯性分析，以確認解決問題的最佳方式。在有些狀況中，這可以減少確認與回應時間達 95%之多。現在，許多 IT 小組可以在不到兩小時內，就將安全威脅隔離，而以前要兩天才能做到。

網路漏洞與防禦攻擊

為了提升安全防禦能見度並降低回應時間，必須建置可以探測網路上不同節點的入侵行為與非法探查漏洞的嘗試之技術。在網路所有進入點與內部網路不同的分界點，建置入侵偵測與預防機制，可以快速偵測辨識異常行為與已知的攻擊，並可以預防安全威脅傷害重要的系統。入侵偵測與預防機制可以確認不同類型的侵入嘗試，而且可以立即通知網管人員有人試圖闖進網路。入侵預防機制可以在這些威脅造成傷害前，就阻止他們的攻擊嘗試。

系統入侵預防機制

作業系統與應用的漏洞會被不同的功擊方式利用，特別是當安全威脅已經避開其他網路層的防禦。一旦一個企業被侵入後，將可能的傷害與損失降到最低，非常重要。這表示必須有機制能快速通知網管人員有網路入侵，在攻擊路徑上提供合適的反擊措施，並預防非法的資訊存取與刪除，或是對網路系統自身造成傷害。網管人員可以更有效的保護伺服器資源，建置終端主機入侵防護機制，協助將「day-zero」安全威脅可能造成的損失降到最小，並預防進一步的攻擊。終端主機入侵預防系統可以避免特定型態的行為發生，包括位元操控、鍵盤側錄、非法使用網路與其他惡意網路行為等。

如何開始

大部分企業都擁有一些工具，可以當成是發展強大威脅預防架構的起點。企業可以隨著安全策略的調整，階段性導入安全技術。企業應該定期檢討其安全控管流程，確保企業採用最佳作法。一個全面性、主動性的安全策略，是一個不停演進的過程；確認其中的關鍵點是重要的第一步。

將既有安全網路基礎架構效能最大化

許多企業都已經建置防火牆與防毒解決方案，這些產品可以在防禦體系統第一線與最後一個關卡發揮作用，提供網管人員關於網路在任何時間無價寶貴的資訊。

- **推薦一**：建置一個安全威脅關聯性分析與警報管理系統，以俾將警報、政策違反與日誌(log)的有效性最大化。這可將把網管人員原本必須花在手動分析網路登入紀錄分析上的時間降到最低，並把安全威脅能見度大幅提升。

思科解決方案：思科安全監控分析與回應系統(Cisco Security Monitoring, Analysis, and Response System; Cisco Security MARS)。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/mars。

- **推薦二**：重新檢視你的週邊安全技術與政策，以確保其可以因應新類型的攻擊，例如異常協定、以應用為基礎的攻擊、與網路入侵等。這不只可以協助因應不斷變化的安全威脅類型，也可以讓網路基礎架構因應無法避免的攻擊類型轉變。因為隨著新網路漏洞的出現，也就會有新的方法來利用這些漏洞進行攻擊。

思科解決方案：思科 ASA 5500 系列自動調適安全應用(Cisco ASA 5500 Adaptive Security

Appliances)解決方案。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/asa。

- **推薦三**：企業應考慮採用那些可以協助濃縮眾多安全建議的服務，以將這些建議針對你的營運與企業需求客製化。這將可以協助網管部門降低檢視從 CERT 或 SANS 等機構所發出的新型威脅警報。如此它們可以專注處理對您的企業有直接影響的安全威脅。

思科解決方案：思科智盾警報管理系統(Cisco IntelliShield Alert Manager)解決方案。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/intellishield。

強化企業遠端據點安全

包括分公司與衛星辦公室、合作夥伴據點、與遠距使用者等的遠端據點，都增加威脅進入企業的機會。無線網路、適當的存取點管制(包括進入據點的管制)、以及未被管理的設備，都可能是企業試圖保護重要資訊與終端系統時，所將面臨的挑戰。

- **推薦一**：建置無線網路認證與非法無線存取點偵測機制，以協助確保未經授權使用者無法隨便進入企業網路基礎架構中。

思科解決方案：思科無線安全解決方案。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/wirelesssecurity。

- **推薦二**：企業可以考慮進行一次無線網路漏洞評估。這樣的評估不僅可以確認無線網路基礎架構中對外曝露的弱點，還可以建議可行的解決方案。

思科解決方案：思科無線網路安全狀態評估。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/securityconsulting。

- **推薦三**：企業應確認終端主機都具備適當的安全防護，並且不會將安全威脅傳送到網路內，感染其他使用者，並成為攻擊與侵入的可能起點。終端主機可能會被防毒軟體與防間諜軟體所無法辨認的威脅所感染。預防這些終端主機不慎安裝惡意的軟體非常重要，以預防這些惡意軟體收集資料後傳給駭客，或執行其他可能會對終端主機與整體基礎架構造成威脅的動作。

思科解決方案：Cisco Security Agent。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/csa。

- **推薦四**：企業應當在分公司建置入侵預防機制，以防止駭客利用遠端據點進入企業網路。入侵預防系統(IPS)可以建置在分公司的路由器上，協助預防未經授權的登入，保護分公司伺服器的基礎架構，免於受害。

思科解決方案：Cisco IOS IPS。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/ips。Cisco IPS 的服務提供持續的攻擊特徵資料庫更新，作業系統與應用軟體更新，以及硬體及軟體的支援服務，可以讓思科的 IPS 解決方案持續更新。

- **推薦五**：企業應建置遠端閘道器具備防毒、防垃圾郵件、防間諜程式等軟體，以保護網路的終端主機與基礎架構，特別是那些未被管理的設備，或是安全管制被使用者關掉的部分。全力清除掉感染惡意軟體碼的傳輸，例如病毒、垃圾郵件、與間諜軟體等，可以大幅改善系統的安全與網路的效能。

思科解決方案：思科 ASA 5500 系列 Anti-X 版本。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/asa。

Day-zero 威脅防護與加強安全威脅能見度

企業應當加強對伺服器、系統與應用程式基礎架構的保護，免於「day-zero」威脅的入侵，並確保企業會遵循相關的安全政策與規範。漸進式改善企業既有的安全技術，可以大幅強化企業的安全狀態。這些改變可以協助提升對於攻擊類型的能見度，協助 IT 小組減少偵測與回應安全狀況所需的時間。

- **推薦一：**檢討並更新入侵與攻擊保護機制，包括偵測已知的攻擊與異常的網路流量。IPS 攻擊特徵資料庫應該被定期檢視；在很多情形中，可以委以第三方 IPS 攻擊特徵資料庫服務執行這項工作。應該與業界同步採取最佳做法，以防止系統漏洞被濫用。企業應該同時進行攻擊特徵與異常行為偵測，以確保最大的安全防禦範圍與最精確的威脅偵測。

思科解決方案：思科 IPS 4200 系列偵測感應器、思科 Catalyst 6500 系列入侵偵測系統模組(IDSM-2)、思科 ASA 5500 系列 IPS 版本。想要了解更多的詳情，請瀏覽：

- 思科 IPS 4200 系列：http://www.cisco.com/go/ips。
- 思科 Catalyst IDSM-2：http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html。
- 思科 ASA 5500 系列 IPS 版本：http://www.cisco.com/go/asa。

- **推薦二：**企業應在伺服器與使用者電腦上，建置終端主機安全防護，以保護系統並提供網管人員安全威脅的詳細資訊。終端主機的異常行為，包括不慎安裝不詳軟體碼、鍵盤側錄、information farming 與移轉等等，都可以被偵測、分析並阻止。系統可以使用同一套安全防護工具，回報安全威脅給中央管理主機，協助確認安全威脅特徵，因此得以大幅改善對安全威脅特徵的辨認度，進一步減少回應時間。

思科解決方案：Cisco Security Agent。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/csa。

- **推薦三：**企業應檢視安全政策管理與安全威脅關聯性技術，以將安全事件發生時回應時間降到最低。由於需要檢視的資料量減少，需要解決安全威脅與侵入的步驟也精簡，網管人員得以縮減回應時間—在有些狀況下，甚至可以減少達 90%之多。協調統合過的安全政策管理與安全威脅管理工具，是達到上述目標很重要的因素。

思科解決方案：Cisco Security Agent、Cisco Security MARS。想要了解更多的詳情，請瀏覽：

- Cisco Security Agent：http://www.cisco.com/go/csmanager。
- Cisco Security MARS：http://www.cisco.com/go/mars。

控制網路存取點與終端主機安全政策

進入內部系統、網路、與應用的存取點，應當僅限於受信任使用者使用，企業在授權終端主機登入內部網路的權限時，必須先確認終端主機的安全狀態。這將可以大幅降低不論是在有意或無意狀態下，安全威脅進入網路基礎架構的可能性。

- **推薦一：**在無線與公共匯集點，建置網路許可控制(Network Admission Control；NAC)。NAC 協助防止在信任的連結上有不慎的登入，並讓所有使用者享有更大的登入彈性。初步應先制定電腦的無線網路存取安全規範；下一步則是擴大到針對所有設備與使用

者，進行更全面的許可控制。

思科解決方案：Cisco NAC。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/nac。

- **推薦二**：檢視週邊防火牆架構，以了解新的網路漏洞。檢視防火牆政策，將應用層級與協定層級的新型威脅納入考慮。網路管理機制應該要容許快速設定新的防火牆政策與存取控制清單，以協助圍堵「day-zero」威脅的發生。

思科解決方案：思科防火牆解決方案。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/firewall。

- **推薦三**：企業應檢視企業區域網路政策並建置整體內部網路的 NAC。有了適當的區域網路保護與周邊控制，再依據使用者身分及存取規定，檢查使用者存取安全政策，針對公司內部網路與公司外部網路使用者，加強許可控制政策。

思科解決方案：Cisco NAC。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/nac。

以系統化方式控制與封鎖安全威脅

為了建置一個有效的安全威脅控管解決方案，思科建議採用完全的生命週期系統化方式。管理網路安全風險與遵循相關法規的最佳方式，就是利用一個系統化、架構性的方式，來因應整個網路生命週期中所面臨的問題，而這樣的方式將是奠基於標準化網路安全的基礎架構之上。思科生命週期服務(Cisco Lifecycle Services)協助企業實現網路與安全技術的最大效益，並可讓企業隨著網路的演進，保持全面性的防護機制。

思科與合作夥伴依據已獲實證的方法與最佳實作，共同推出許多服務，讓企業可以建置經有效設計、安裝、管理、並可以整合入整體基礎架構與營運流程的安全控管系統。

- **推薦一**：思科安全服務可以讓企業了解網路目前的安全強處與脆弱處，採用許多不同方法來評估網路預防、偵測、與解除安全威脅的能力。漏洞評估與安全架構檢視，是確認系統與網路層級脆弱漏洞的有效工具。

思科解決方案：思科安全狀態評估與安全架構檢視服務。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/securityconsulting。

- **推薦二**：企業應依據深入整體系統的方法以及被業界接受的標準，來規畫與設計一個安全威脅控制系統。一個強大的設計與整合架構，可以提升安全威脅控制解決方案有效度，縮短建置時間，降低整體整合成本。思科提供專業協助，以發展一個強大的安全威脅控制設計。

思科解決方案：思科安全設計服務。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/securityconsulting。

- **推薦三**：企業應依據對整體安全架構的認識，建置、設定、並將新的安全威脅控制系統整合入網路整體基礎架構。多層的防禦機制是必須的，但是這可能會增加網路安全管理的複雜度，更難確認與解決安全威脅。思科具備完善的網路整合專業，可以加速安全威脅控制解決方案的成功導入。

思科解決方案：思科安全建置服務。想要了解更多的詳情，請瀏覽 http://www.cisco.com/go/

securityconsulting。

- **推薦四：**企業應當主動管理 IT 基礎架構，快速並精確的預測、確認、與解決安全威脅。安全威脅控制系統應該包含及時、精確、與可信賴的安全智慧機制，並與安全威脅關聯性及警報管理系統結合。企業也應考慮採用遠距管理服務，主動管理安全威脅控制基礎架構。思科解決方案：思科智盾警報管理員、思科 IPS 服務、思科遠距管理服務。想要了解更多的詳情，請瀏覽：
  - 思科智盾警報管理員：http://www.cisco.com/go/intellishield。
  - 思科 IPS 服務：http://www.cisco.com/en/US/products/ps6076/sev_group_home.html。
  - 思科遠距管理服務：http://www.cisco.com/go/ros。

總結

安全威脅的面貌已經轉變，網管與安全管理團隊也必須能控制眾多不同的網路基礎架構安全威脅，而且還須同步確保網路存取安全給有需要的使用者。關鍵在於，在安全事件發生時，企業要能夠管理大量的警報與資訊，並將損害降到最低。也因此，網管與安全營運團隊，都面臨減少危機回應時間的壓力。

從病毒、網路詐騙釣魚、網路攔截到入侵，安全威脅的演進與複雜度必須被重視，必須讓網管部門可以依據整體網路基礎架構所提供的情報，快速做出決策。網路本身也必須提供精確詳細的安全威脅分析，並必須可以預防、偵測與解決新型與已知的安全威脅，以協助減輕網管部門資訊超載的負荷，縮短回應與解決安全威脅的時間。思科自我防衛網路與思科安全威脅解決方案，將可協助網管部門因應持續變遷中的網路安全威脅，並解除這些安全威脅企圖造成的損害。

台北總公司
台北市信義路四段 460 號 12 樓
www.cisco.com.tw
Tel：02 - 8758 - 7100
Fax：02 - 8758 - 7199

台中辦事處
台中市公益路二段 51 號 20 樓 A2
www.cisco.com.tw
Tel：04 - 2327 - 1372

高雄辦事處
高雄市苓雅區三多四路 110 號 19 樓之 2
www.cisco.com.tw
Tel： 07 - 338 - 1092
Fax： 07 - 338 -1094

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**