

發展完整可管理之威脅控管策略

執行摘要

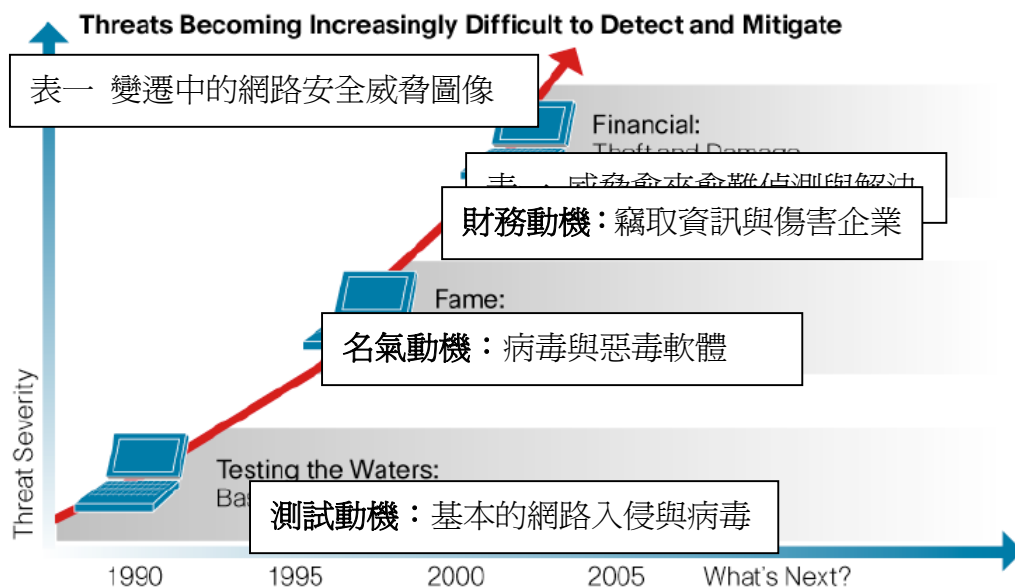
任何對網路安全的破壞，都會讓網路攻擊所鎖定的企業，遭受重大災難。網路漏洞可以嚴重危害企業運作與生產力，導致智慧財產權被竊與財務損失，並可能危及法令規範的施行。不幸的是，近年來駭客攻擊的次數與複雜度，愈來愈嚴重，讓網路管理工作與企業面臨的潛在風險，變成更大的難題。

為了抵禦網路攻擊，企業必須建置網路安全機制，可以主動偵測並回應既存與即將發生的威脅。這些解決方案必須讓網路與管理機制的每個部份，都可以協同保護網路基礎建設，解決各種不同的安全問題，且同時可以降低回應與解決問題時所需的時間。這樣的策略可以協助企業維護業務的連貫性，讓整個網路基礎建設具備探測威脅的能見度與保護機制，並可以簡化網路安全政策與系統管理。

思科自我防衛網路解決方案 (Cisco Self-Defending Network Solution) 中的重要關鍵套件思科威脅控管解決方案 (Cisco Threat Control Solution) 可以協助企業反制既有與潛在的安全威脅。有了這個完整的解決方案，企業可以主動保護他們的網路系統，簡化網路管理並改善業務的連貫性，讓他們可以更專注在業務目標上，而不是在網路安全上。

全新網路安全版圖

在過去幾年內，駭客創造病毒、破壞系統、搗亂網路通訊的主要動機因素，就是為了吸引媒體與駭客同儕的注意。然而，今日的駭客更感興趣的卻是如何從中牟取財務利益 (見表一)。由於有利可圖，駭客開發出一系列有害的新興網路攻擊機制，其感染網路系統的速度，比軟體與作業系統供應商開發的補丁與臨時解決方法還要快速。特別設計以規避安全偵測並繞過傳統防禦系統的許多新興技術，讓許多企業在未準備下驚慌失措。新興開發出來的網路垃圾與類似網路釣魚 (phishing) 等詐騙手法，讓沒有警戒心的使用者，在毫不知情下揭露了私人與敏感的訊息。

Figure 1. The Changing Threat Landscape


表一 改變中的網路安全威脅圖像

由於網路安全環境不斷改變，企業被迫花上比以前更多的時間與資源在網路安全上面。然而，許多企業使用的技術卻缺乏可以適當保護網路與減輕 IT 人員負擔的必要能力，而這些 IT 人員早已因為要求支援的電話、定期維修、與每日的維護工作而造成負荷過重。

許多公司經常導入單點的產品，例如入侵防護系統 (IDS)、防火牆、以及內容安全技術 (例如防毒軟體、防垃圾郵件軟體、與防間諜軟體等)。但是多個單點的產品通常缺乏提供完整保護所需的整合性。除此之外，單點產品與標準安全解決方案，通常都缺少系統性檢查每個網路安全元素、區域及設備的精細度。但這種系統性層級的檢查能力是必須的，因為駭客鎖定的網路侵入點與種類不僅多樣化而且還在持續成長中。這些威脅包括：

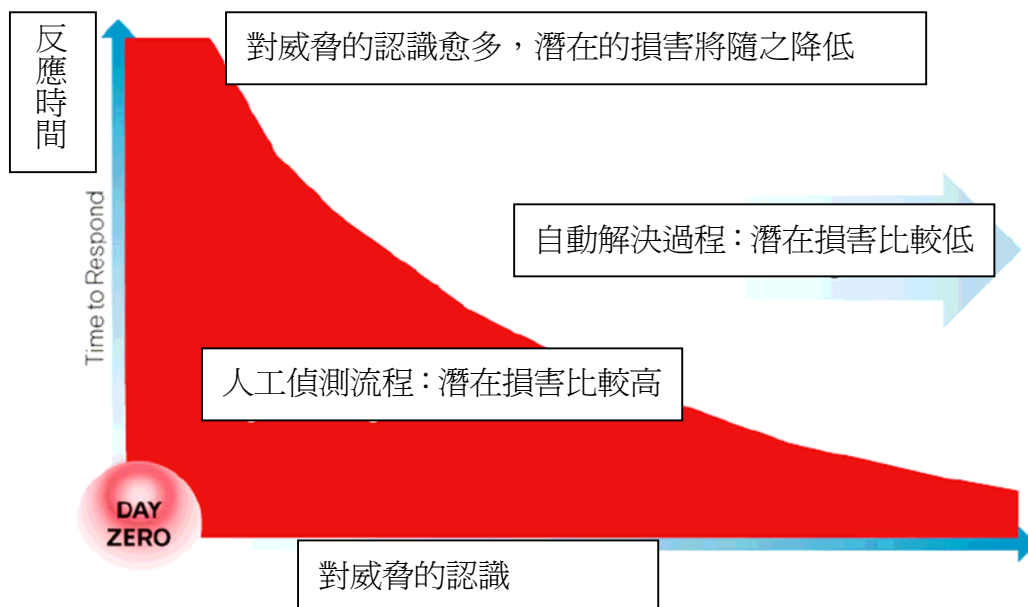
- ◆ 商務溝通：電子郵件、網站、資料傳輸、即時通訊、與其他商務與個人通訊的標準形式，都可能帶來許多不同的網路威脅，可以重創無防備的使用者。
- ◆ 行動設備與桌上型個人電腦：網路對於來自行動設備與桌上型個人電腦、不安全的無線上網、與被竊筆記型電腦的病毒感染，抵抗力相當脆弱。
- ◆ 免費軟體與共用的媒體：惡毒軟體會藏在類似像 CD 或 DVD 這樣的媒體，並隨之傳播出去，可以因此躲過安全控管，在其他系統中被執行或複製。

提供 360 度的防禦

在當今惡意網路攻擊威脅日益嚴重的環境中，企業需要一個智慧型、從前端到後端完整的解決方案，讓網路安全的元素可以整合至所有的設備、伺服器、作業系統與終端單點。隨

著網路安全緊密連結在一起，所有的管理系統、加強節點、與主控點(host)都可以共同合作，主動的調整以回應即將發生與立即可見的威脅。終端單點、網路與管理的協同合作，將可以讓這樣的系統比單一平台回應更快速，保護更完善（見表二）。

Figure 2. Benefits of an Intelligent Security Solution



這樣一個解決方案可以強化對網路上所有的溝通、活動、與事件的偵測能力，改善 IT 人員下決策與管理政策的能力。在安全事件發生時，當系統、網路與主控點大量發出威脅警報，這樣的解決方案將可大幅減低此時所需的人為回應。在一個時間處理一個警報，會讓 IT 小組負荷過重，也讓標準的工具變得無效率，最後終致幾乎無法即時找到威脅來源。然而，一個整合的解決方案可以透過確認威脅類型、將關聯性的事件歸納入不同的風險種類、以及確認最佳的解決方式，將安全系統的效能極大化。

思科發現在某些狀況下，一個整合的防衛系統可以降低確認威脅與回應的時間，減少時間幅度甚至可高達 95%。許多 IT 組織都指出，他們已經可以在不到 2 小時之內，就可以將威脅隔離。但若是沒有這樣的解決方案，通常要 2 天的時間才能完成。

如何跨出第一步

一個完整的安全策略需要不斷的警覺性與持續性的修正。透過確認關鍵性的安全重點，包括安全系統、使用政策、回應政策、緊急應變計畫、以及個別資產的風險程度，組織可以在這個演進過程中，跨出重要的第一步。

一旦完成了評估之後，企業可以開始導入「思科威脅控管解決方案」(Cisco Threat Control Solution)。許多企業已經擁有一些工具，可以由此出發，來發展一個強大的威脅預防架構。隨著公司改變，安全策略也隨之調整，企業可以隨此而階段性引進其他技術。企業也應定期檢視其網路安全流程，以確保組織遵循最佳的作法。

「思科威脅控制解決方案」重要元素

「思科威脅控制解決方案」使用一個完整的安全技術套件，以保護網路免於來自網路內部或外部的攻擊與侵入。「思科威脅控管解決方案」提供對整體 IT 架構深入的能見度與控制，簡化威脅管理的執行，並協助確保企業的營運彈性。然而，要建置一個完整的安全解決方案可能有其困難度，尤其想要畢其功於一役更困難。因此，思科推薦的是一個漸進的方式。在建置一個威脅控管解決方案時，企業應該在導入可以強化保護的額外元件前，以下面三種技術為基礎來考量：

- ◆ 思科安全監視、分析與回應系統 (Cisco Security MARS)
- ◆ 思科入侵保護系統 (Cisco IPS)
- ◆ Cisco ASA 5500 系列調整型安全應用 (Cisco ASA 5500 Series Adaptive Security Appliances)

思科安全監視、分析與回應系統 Cisco Security MARS

今日的 IT 管理者需要看到網路狀況的清楚圖像，以便做出有效的決策，採取恰當的防禦行動，像 Cisco Security MARS 這樣一個威脅相聯性與警報管理系統，可以大幅改善威脅的能見度，降低控制警報並找到威脅進入點的人工時間，將安全意外造成的傷害最小化。

Cisco Security MARS 是一個以應用為基礎的完整解決方案，對於既有的安全系統，可以提供更佳的深度了解與控管。Cisco Security MARS 是思科網路安全管理生命週期解決方案中的重要元素，可以與既有的網路與安全系統相容，以確認、隔離、管理並建議將入侵元素精確的移除。這個解決方案將未經處理的網路與安全資料，轉換成可以用來破解具體安全事件的情報。這個簡單易用的危機化解應用產品系列，可以讓系統管理員中央化管理企業架構，統一偵測、化解並回報在既存第三方、與思科的網路與安全設備上，所發現的最危急威脅。Cisco Security MARS 還可協助維護企業內部對政策與規定的遵守。想要了解更多關於 Cisco Security MARS 的詳情，請瀏覽 <http://www.cisco.com/go/mars>。

思科入侵保護系統 (Cisco IPS)

今日的企業必須抵禦由於異常網路協定、應用端的漏洞或網路入侵所造成的經常性網路攻擊威脅。Cisco IPS 可以保護伺服器、終端單點、與重要的基礎建設免於攻擊，以及來自於其他應用與作業系統的資源剝削行為。預防入侵是一個成功網路安全解決方案中重要的一個元素，因為它可以偵測並阻止包括像軟體病蟲、網路病毒與其他惡毒軟體等的攻擊。

Cisco IPS 利用下面的方式，提供領先業界的保護能力：

- ◆ **普及的網路整合：** Cisco IPS 從不同的地方擊敗威脅，包括網路、伺服器與桌上型電腦終端單點。它從第二層到第七層都詳細的檢查，以保護網路免於違反政策、因漏洞而被濫用、與惡質活動。Cisco IPS 在思科許多平台上皆可使用，包括 Cisco ASA 5500 系列調整型安全應用。
- ◆ **協同預防威脅：** Cisco IPS 採用獨特的系統，可以協同評估威脅並做出回應，具備強大的網路擴充性與彈性。Cisco IPS 的功能包括跨解決方案的回應連結、共同政策管理、多重供應商事件相連性、攻擊路徑確認、被動/主動指印、與以主控者為基礎的協同合作。
- ◆ **主動型態調整：** 隨著網路威脅型態改變，Cisco IPS 也隨之演進並調整，以解決來自

已知與未知來源的威脅。廣泛的行為分析、異常狀況偵測、政策調整、與快速威脅回應技術，可以節省時間、資源與組織的資產與生產力。

想要了解更多關於 Cisco IPS 的詳情，請瀏覽 <http://www.cisco.com/go/ips>。

Cisco ASA 5500 系列調整型安全應用 (Cisco ASA 5500 Series Adaptive Security Appliances)

維護系統安全需要可以防衛不同攻擊的閘道器技術。系統必須能夠確認異常的協定、以應用為基礎的攻擊、與入侵方式。「Cisco ASA 5500 系列調整型安全應用」正是這個問題的答案，提供中小企業對於其系統的控制與彈性，以協助防禦快速演進的威脅。

這個高效能的系列平台將同級最佳的安全與虛擬私有網路 (VPN) 服務，以及一個可延展的創新服務架構結合起來，提供主動防禦措施，讓企業得以在威脅散播在整個網路之前就先主動制止，並讓企業可以控制網路活動與應用流量，給予企業彈性的 VPN 連結性。Cisco ASA 5500 系列採用全功能、高效能的防火牆、侵入預防、內容安全、與安全套接層/IP 安全(SSL/IPSec) VPN 技術等，提供強大的應用安全功能、以使用者與應用為基礎的網路擷取管制、病蟲與病毒的解決、惡毒軟體的防護、內容過濾、以及遠端使用者/網站的連結功能。

Cisco ASA 5500 系列將既有的服務最佳化，並讓企業得以建置新的服務，但卻不必更換平台或是把效能打折扣。該解決方案提供高度有效的政策架構，並透過使用者可建置安全服務模組 (SSMs) 與安全服務卡 (SSCs)，結合軟體和硬體擴充性。除此之外，該解決方案還具備平台、設定與管理標準化的功能，可以協助降低系統建置與後續營運的成本。

想要了解更多關於 ASA 5500 系列產品的詳情，請瀏覽 <http://www.cisco.com/go/asa>。

其他選項

組織應該考慮採用外包的解決方案，來管理那些每天都會把網路系統灌爆的警報與系統事件。思科所提供的服務，可以將眾多安全諮詢建議，精煉取其精華，改善企業利用網路的能力，以俾滿足業務與組織上的需求。這可以把花在檢視來自於像社群緊急應變小組 (CERT)、系統管理員、稽核、網路、安全 (SANS) 機構等團體的警報時間縮到最短，讓 IT 部門得以專注於將會直接影響公司的威脅上。思科的解決方案就是：思科智盾型警報管理者 (Cisco IntelliShield Alert Manager)。想要了解更多關於詳情，請瀏覽 <http://www.cisco.com/go/intellishield>。

總結

企業安全威脅的圖貌發展，比起前幾年來，已經越來越加危險，安全管理也因此變成更大的問題。IT 與安全管理人員已經因為安全系統持續發出愈來愈大量的安全警報與資料而負荷過重，比起以前他們需要管理的風險範圍愈來愈廣，網路也愈來愈脆弱，但是他們卻不能阻止有權上網的使用者使用網路。而這對企業的潛在損害，會讓每個不可避免的危機都更快發生。

為了確保快速解決這個問題，網路本身必須提供準確細節的資料與威脅分析。這將可協助 IT 人員預防、偵測、與解決潛在與明確的威脅，調節資訊容量過多問題、並降低回應與解決所需的時間。思科提供一個完整的、端點對端點的解決方案，可以有效的管理今日網路安全的風險，讓企業可以把潛在性的損害降到最低。有了思科威脅控管解決方案，網路安全與重要商務溝通將持續處在安全與營運狀態，而員工也可以持續維持他們的生產力。



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.

 ©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCOE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco System Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609F)