

為何選擇威脅控制與圍堵方案？

網路安全威脅會嚴重影響生產力，導致企業營運與業務中斷，以及資訊的流失，這不僅將導致企業面臨財務損失，亦會因此違反相關法規規定。駭客不斷發展新的技術來擷取資訊，獲取金錢利益，這些技術比以往更難偵測。企業需要完備的解決方案，具備優異的管理功能與運作效率，能主動克服這些威脅。

需要解決哪些問題？

企業面臨錯綜複雜的安全問題，像是：

- 面臨病毒或蠕蟲攻擊時，員工與 IT 部門的生產效率
- 機密資訊的安全性
- 保護企業的聲譽與品牌
- 通訊中斷以及對日常營運的影響
- 電子商務應用的持續運作

實際威脅影響實際網路的範例

- 用來偽造信用卡的 Zotob 病毒：遭受 Zotob 蠕蟲攻擊的機構包括 CNN、ABC News、紐約時報、波音公司，因此美國國土安全部努力對抗信用卡偽造犯罪。FBI 相信 Zotob 的發明者可能受雇撰寫超過 20 種其他病毒。
- 竊取金錢的「rxbot 木馬程式」：所謂的「rxbot 木馬程式」已經感染了 40 萬部裝有 adware 程式的電腦，發明者藉此從點選廣告軟體製造商獲得超過 6 萬美元的獎勵金。被指控的發明者於 2005 年 11 月被捕，被控攻擊數千部主機，包括美國海軍空戰中心武器部門的電腦，以及美國國防部國防資訊系統局的電腦。
- 竊取商業資訊的顧客導向木馬程式：顧客導向木馬程式的設計人，其目的是創造與散佈間諜程式，藉以取得商業資訊，並把程式賣給私人調查公司。這些公司利用間諜程式從客戶的競爭對手竊取資料。根據警方的報告，這類程式利用作業系統的防禦弱點，透過標準資料擷取方法，包括側錄鍵盤輸入鍵、擷取螢幕畫面以及檔案傳輸等。警方指出這種木馬程式透過電子郵件或送至目標企業的磁碟進行植入，據許多受害者回報，感染的管道包括熟知或可靠的商務聯絡途徑。包括美國與歐洲在內數十家企業都曾受害。

威脅控制與圍堵解決方案

Cisco的威脅控制與圍堵解決方案為顧客提供一個完備的方案，以用來控制與圍堵各種安全威脅，提供無與倫比的保護，讓所有規模的組織機構免於遭受網路與鎖定式攻擊和入侵。

- 360度全方位的可見度與保護：提供完備與主動式的網路防禦機制
- 涵蓋整個基礎架構的威脅掌控能力，以低廉的成本支援各種系統與裝置
- 多層面的威脅辨識，找出違反策略、防禦弱點以及異常行為
- 簡化的控制：加快整個網路的策略執行與管理
- 讓各種網路元件的策略管理加以標準化
- 涵蓋整個基礎建設的建置，支援各種系統與裝置
- 業務持續性：確保企業的業務持續運作
- 無與倫比的協同分工與連結功能，涵蓋各種系統、端點以及管理程序
- 針對各種即時威脅，進行調適性的反應
- 思科自我防禦網路策略的核心元件

威脅控制與圍堵解決方案的核心元件

- Cisco ASA 5500 系列Adaptive Security Appliances—模組化平台提供新一代的安全與VPN服務，支援各種環境，從小型辦公室一直到大型企業。<http://www.cisco.com/go/asa>
- Cisco ASA 5500 Anti-X Edition—從閘道器抵禦各種網路安全威脅，包括間諜程式、垃圾郵件、病毒以及其他和網路內容有關的安全威脅。<http://www.cisco.com/go/asa>
- Cisco Security MARS—提供安全威脅管理介面，將網路與安全資料整理成可派上用場的資訊。<http://www.cisco.com/go/mars>
- Cisco 入侵防禦系統(IPS)解決方案—保護伺服器、應用、以及其他關鍵資產免於遭受網路與應用軟體攻擊與感染蠕蟲，保護範圍涵蓋閘道器、分支據點、資料中心、以及整個區域網路。<http://www.cisco.com/go/ips>
- Cisco Security Agent—保護伺服器與桌上型電腦免於各式攻擊，包括：間諜程式入侵、取得 root 身份的入侵程式以及零日攻擊 (day-zero attack)。<http://www.cisco.com/go/csa>
- Cisco Network Admission Control (NAC)—透過檢驗使用者與系統的安全憑證，保護網路與基礎設施免於遭受感染。<http://www.cisco.com/go/nac>
- Cisco Security Center 入口網站提供單一整合化的來源，針對目前各種安全事件提供指示，包括如何運用思科產品與服務來對抗新型威脅。

針對威脅控制與圍堵解決方案提供的生命週期安全服務

Cisco Security Center 入口網站提供一個整合來源，介紹當前最新的安全事件，包括如何運

用思科產品與服務來抵禦各種安全威脅。

Cisco IPS Signature Subscription 顧客可存取 Cisco Security IntelliShield Alert Manager 資料庫，針對各種 IPS 事件提供完整的資訊，並能將 IPS 特徵連結到 IntelliShield，藉以加快對抗攻擊的速度。

Cisco IPS、Cisco Security MARS、Cisco NAC 以及 Cisco Security Agent 建置諮詢服務能簡化各種新解決方案的建置流程，由思科專家運用合理的安全設計原則，提供網路整合方面的專業知識。

Cisco IPS 遠端更新與調校服務能簡化各種 IPS 裝置的日常運作，在特徵更新資料發佈後，立即進行部署與調校。

從何著手？

大多數組織都已有相關工具，可以此做為起點，逐步建構一個完善的威脅防禦架構。隨著企業持續修正安全策略，企業可分成數個階段，逐步採用適合的技術。安全流程可定期檢討，以確保組織採用最佳的策略。一個完善、主動出擊的安全策略，是一個持續演進的流程；第一步就是找出關鍵點。請參考思科威脅控制與圍堵白皮書，您可向思科人員索取，這本白皮書詳列如何推動安全解決方案的下個發展階段。

為何選擇思科？

思科是全球網路安全解決方案的領導者。思科提供最廣泛的能力，能協助整個 IT 基礎架構抵禦各種安全威脅，從端點、網路、一直到管理層。思科的整合、分工、以及調適性安全解決方案，協助對抗組織現今面臨的各種安全威脅，協助確保 IT 與員工的生產力，及保護組織最重要的資訊資產。從網路威脅、鎖定對象的攻擊與入侵，思科的解決方案為 IT 與安全管理者提供他們需要的工具，在現今日趨複雜、難以抵禦資訊安全威脅的時代，有效保護其組織機構。



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)