# 透過 Cisco 統合無線網路的整合式無線 IDS 與 IPS，解決無線網路通訊威脅

**這份報告旨在討論惡意 AP(Rough Access Point)與其他威脅對網路所造成的影響，以及 Cisco 統合無線網路將如何偵測與防禦這些問題。**

## 摘要

自從 1997 年 IEEE 802.11 問市之後，無線區域網路（Wireless LAN, WLAN）的安全已大幅改善。隨著最新的安全標準 IEEE 802.11i 推出後，WLAN 就像許多有線網路一樣、甚至更為安全。然而，由於無線區域網路範圍超出企業辦公室，無線網路的安全威脅，便會來自未經授權的基礎建設與客戶。對 IT 管理者來說，好消息是 Cisco 統合無線網路（Cisco Unified Wireless Network）解決方案可以偵測與防禦這些威脅，並同步提供無線網路客戶所需的服務。還不想建置無線區域網路系統的企業，可以選擇採用 Cisco 統合無線網路，利用監控模式以確保無線網路威脅不會危及有線網路的完整性，導致機密資料的遺失、客戶信心降低、或造成可能的違法行為。

## 挑戰

雖然 IT 管理者可能已經知道利用 IEEE 802.11i 來保護無線區域網路的適合技術，但他們可能還是會很驚訝的發現，即便這樣仍不足以維護企業安全。不論企業是否有授權的無線區域網路，或是沒有 Wi-Fi 的政策，企業必須瞭解即使是層層防護的企業網路，在無線網路威脅下仍有其脆弱性。最常見的威脅就是惡意 AP。迫切需要上網的員工常將自己的 AP 帶到公司，利用一般消費型等級而且低價的 AP，以加速在部門內部的無線連結，但他們卻不理解其中的危險性。這些惡意 AP 通常可以躲過防火牆，不會被傳統有線網路一般使用的入侵偵測或是入侵防禦系統偵測到（Intrusion Detection System/ Intrusion Prevention System, IDS/IPS）。在訊號範圍內的任何人，都可以連上此 AP 並進入該企業網路。

由於行動工作者不論在公司內部或外部都要可以上網進入公司內部網路的要求，讓安全挑戰更為複雜。企業員工經常會在家裡、旅館、機場、以及其他無線上網熱點上網工作。由於筆記型電腦有感染病毒、間諜軟體、與惡毒軟體的風險，這些未被管理的上網點都將成為威脅進入企業網路的通道。無線網路客戶在連結至無線 AP，或是缺乏無線使用知識的情況下，都會使問題嚴重惡化。

## 解決方案

Cisco 的自我防禦網路（Self-Defending Network）策略可以保護企業網路安全，免於來自無線技術的威脅。結合 Cisco 整合安全解決方案（Integrated Security Solution）， Cisco 統合無線網路將提供企業全面性的解決方案，可以保護企業有線網路免於無線網路威脅，

並確保授權無線區域網路上安全、機密的通訊。在這個網路上的每個設備—從客戶、AP 到無線控制器與管理系統，都在分配式防禦機制中各司其職，確保無線網路安全。這份報告將解釋不同的無線網路威脅，以及 Cisco 統合無線網路如何整合自動無線網路入侵偵測與防禦，以保護企業安全。想了解確保你無線區域網路安全的五個重要步驟，請參閱「確保無線區域網路安全與防禦無線網路威脅的五個步驟」報告。

## 建立準確的威脅偵測與防禦

建立準確威脅偵測與防禦的第一步，就是要確保無線基礎架構有授權機制，所有使用者也必須獲得適當認證才能進入網路。少了這個步驟，任何的 IDS/IPS 價值都將難以發揮，因為網路管理員必須花費許多時間解決錯誤的警報。IEEE 標準透過 802.11i 認證，可以精準地確認獲授權客戶與基礎架構的身分。

IEEE 802.11i 安全標準利用 IEEE 802.1X 技術，以執行網路與客戶間的相互認證。也就是說，任何想要利用網路資源的客戶，都需要經過網路認證。同樣地，客戶也會先確認所加入之網路基礎架構的真實性，才會開始進行資料傳輸。有了 802.1X 標準，認證所需的如登錄密碼等資料，若未被加密就不會透過無線網路傳輸出去。除此之外，802.1X 提供每個用戶、每次上網的動態加密金鑰，以減輕行政管理上的負荷，與減少靜態加密金鑰相關的安全考量。

雖然 802.1X 認證形態可以提供無線區域網路強大的認證功能，但是嚴謹的加密技術仍是必須的。原始的 802.11 標準包括有線等效加密(Wired Equivalent Privacy, WEP)加密技術，但它對網路攻擊的抵抗性弱，現今企業都應避免使用。為了彌補 802.11 與 WEP 的這個缺點，以及 802.11i 安全標準的延遲批准，Wi-Fi 聯盟訂定了一個業界標準，稱為 Wi-Fi Protectes Access (WPA)。WPA 利用 802.1X 的認證技術與暫時金鑰整合協定(TKIP)加密技術。

在 2004 年，IEEE 終於批准了 802.11i 無線區域網路的安全標準，包括 802.1X 認証與先進加密標準(Advanced Encryption Standard, AES)加密技術。Wi-Fi 聯盟主推可相互操作的 802.11i 認證，則被稱為 WPA2。WPA 所使用的 TKIP 加密演算法十分強大，但卻還是不如 AES，應該僅被當成是過渡性的安全政策，直到客戶升級能夠使用 WPA2 與 AES。只要情況許可，Cisco 強力推薦採用 WAP2 與 AES 來打造最強的安全環境。

## 檢視常見無線網路威脅

一旦授權的使用者與基礎架構被認證， Cisco 統合無線網路將可以保護企業免於常見的無線網路威脅。Cisco 統合無線網路輕量級 AP 可以同步控制無線客戶流量並監控其空間，或是可以當成專屬的無線監控器。本文將於常見無線網路威脅的討論之後，深入介紹關於 Cisco 統合無線網路的先進安全服務。

## 惡意無線接入點與客戶

最常見的無線網路威脅就是惡意 AP。惡意 AP 通常是被想要隨時無線上網的員工帶入企業內部網路的。這些通常是低價與消費型產品等級的 AP，在有線網路上通常不會被發現，只

能在空中才會被偵測到。由於員工一般是在預設值模式下安裝這些 AP，因此認證與加密通常不會被啟動。由於無線區域網路信號可以穿越建築物牆壁，從開放式 AP 進入企業網路，但卻未被偵測到的情況並非過份誇大。任何連上惡意 AP 的客戶，都必須被懷疑有不良企圖，因為它是繞過 IT 部門規定的安全授權流程而進入公司網路的。

## 特殊網路

特殊網路（Ad Hoc Network）是指兩個客戶設備間直接形成的網路。特殊網路之所以會對企業造成威脅，是因為它可以避開基礎網路架構所執行的安全檢查。其中的危險之一，就是員工可以將能夠無線上網的筆記型電腦帶入公司，連上辦公室的有線網路，啟動無線網路介面。在這樣的情況下，在附近的駭客將可以直接連上客戶裝置，造成安全威脅。同時駭客也可以搜尋員工客戶裝置上的資料，並且可能同步透過無線與有線介面，以進入公司內部網路。這將會使得企業違反產業的規範政策。

## 客戶錯誤連結

無線網路客戶的好處，就是可以快速、容易地加入其他開放網路。然而，這樣的便利對企業來說卻可能是一個潛在的危機。當電腦在執行微軟 XP 系統時，這樣的狀況經常發生。在此情況中，無線網路的設定軟體會自動連結到以前曾經使用過的服務套組確認器（Service Set Identifiers, SSID）。如果這個員工曾經連結至熱點或是家中的 AP，而電腦在公司內讀到同樣的 SSID 時，電腦將會在員工不知情的情況下，自動連結到另一個未知的 AP。如果上述情況是員工在透過有線上網進入公司網路的時候發生時，則可能有不知名人士利用無線網路介面當作進入企業有線網路。或是，員工可能會利用鄰近的無線網路，試圖擺脫內部網路對於電子郵件、即時通訊、或網路使用政策的安全控管。這兩個例子都將會讓企業違反業界的規範政策。

## 阻斷服務攻擊與滲透嘗試

阻斷服務攻擊(Denial-of-service attacks, DoS Attacks)是另一種企業可能面臨的威脅。在阻斷服務攻擊中，並非資料或網路暴露在未獲授權人士面前，而是駭客試圖中斷網路服務。另外一個重要的差異在於，惡意 AP、客戶錯誤連結、與特殊網路都是員工無意造成的，但是阻斷服務攻擊卻是需要特殊技術知識與計畫，因此幾乎都是惡意的舉動。在阻斷服務攻擊中，駭客通常會從客戶設備所連結的 AP 開始愚弄網路訊框，然後再使連結到此 AP 的無線區域網路取消授權(de-authenticate)、或是取消結合(disassociate)。這些攻擊之所以會發生是因為無線區域網路並不像乙太網路，它需要管理架構來管理媒體存取與避免抵觸。因為管理架構需要在客戶設備完成認證之前就被啟動，這些管理架構永遠都是未經認證與加密的，即便是使用 WPA、WPA2、或是 VPN 也是一樣。

事實上，企業網路中很少見到阻斷服務攻擊。因為這些攻擊是透過無線進行，幾乎不可能在駭客攻擊、癱瘓整個無線區域網路之前，網路還沒有發覺他們的實體存在。然而，隨著愈來愈多重要的行動服務問世，例如透過無線區域網路使用語音通話，要能快速確認阻斷服務攻擊並準確地找出攻擊，變得愈來愈重要。

滲入嘗試(penetration attempt)有兩種，一種是中間人攻擊(man-in-the- middle attack)，一種是離線字典攻擊(offline dictionary attack)。中間人攻擊試圖將一個客戶設備從一個合法的 AP 去除，然後讓它連上一個仿獲授權 AP 的惡意 AP。攻擊者將會再嘗試取得客戶的認證資料，並使用這些資料透過無線區域網路進入企業內部網路。

離線字典攻擊則是在空中攔截無線網路上的資料，並試圖破解加密金鑰。攻擊者只需在目標附近，就可以擷取空中的資料，然後在另一個地點，破解加密金鑰。如果他們成功破解，就可以利用加密金鑰進入企業網路。不過，建置 WPA 或 WPA2 安全技術的無線區域網路，將不會被這樣的攻擊侵入。

## 偵查探測

另一種威脅發生的狀況是，有人蒐尋開放的 Wi-Fi 訊號(這被稱作 war driving)，通常他們會使用一種稱為 NetStumbler 的常見工具。一般來說，由於無線網路會將自己的網路名稱或是 SSID 加以透露，這種 NetStumbler 以及其他類似的工具便有機可乘。NetStumbler 通常會利用無線客戶的手持裝置，以不明顯的方式尋找發掘無線區域網路。這是一個典型的被動式工具，但是有時它會主動透露，以致於侵入偵測系統會探測到它。

有些供應商為了推銷專門用來偵測無線網路侵入的系統，會特別誇大網路名稱會被找到的可怕的情況。其實這樣的恐懼是不需要的。建置了 802.111(WPA2) 或 WPA 安全技術的無線區域網路，將不會只因為網路名稱被發覺而被攻擊侵入的。

## 了解被動與主動攻擊

除了了解不同種類的威脅外，了解攻擊的類型也非常重要。也就是說，必須了解特定攻擊是主動還是被動，若是主動攻擊，則需分別是線上還是離線攻擊。

在被動攻擊中，攻擊者並不會與網路進行互動，但是會觀察資料並試圖侵入網路，只為了分析所擷取的資料。被動攻擊的例子包括偵查探測與離線字典攻擊。尤其是在無線區域網路中，因為資料是在空中傳輸，我們很難對這種類型的攻擊做任何處理。防禦這種類型攻擊的最佳防禦措施就是使用功能最強的安全防護。因此，Cisco 建議採用 WPA2 與 AES 技術，以創造最安全的環境。網管人員可以確保在採用 WPA2 與 AES 技術的無線區域網路，沒有任何離線字典攻擊會成功侵入。

主動攻擊是指駭客與網路的即時互動。這類的例子包括惡意 AP、中間人攻擊、與阻斷服務攻擊等。主動攻擊可以進一步再區分為線上與離線攻擊。主動線上攻擊是指那些在無線區域網路提供服務的通道上所發動的攻擊。阻斷服務攻擊是一個很好的例子，因為它們必須與客戶在同一個通道上，否則無法阻斷服務。在這種狀況下， Cisco 統合無線網路的無線 IPS 功能將可提供全天 24 小時、甚至是一周七天的線上保護，因為 Cisco 無線網路控制器都會即時檢驗每個封包。

主動離線攻擊是指那些在其他通道上發動的攻擊，也可包括類似惡意 AP 的攻擊。Cisco 統合無線網路輕量級 AP 可以設定掃描所有的無線通道，確保偵測到線上與離線的攻擊，以防堵威脅。

## 保護無線區域網路覆蓋不到的分公司與其他據點

許多企業都有分公司、遠距辦公室，或是企業總部內無線區域網路覆蓋範圍內的地方。某些時候，這些地方在面臨無線網路威脅時還更脆弱，因為員工可能會將自己的無線 AP 帶到公司以獲得無線上網。為了保護這些地方，企業可以建置 Cisco 統合無線網路輕量級 AP，專門用來進行空中監控。空中監控並不提供客戶的流量服務，僅是負責監控空中的無線波段。所有的通道都將被掃描檢驗，侵入防禦技術也將依需要狀況而啟動，以保護企業安全。

在這種情況下，採用 Cisco 統合無線網路比起一個覆疊的無線 IDS 系統，好處在於當企業準備在這些地點建置無線區域網路時，這些空中監控器可以轉為服務無線客戶；或是如果企業希望針對無線網路威脅有專門的感測網路時，額外的 AP 還可以被同樣的控制器所管理。不論是哪種狀況，企業都只需要建置、學習使用、與定期維護一個系統。

## 利用 Cisco 統合無線網路，偵測與防禦無線網路威脅

下面的文章將說明不同的策略，讓您使用 Cisco 統合無線網路以偵測與防禦無線網路威脅。

## 使用無線電資源管理以偵測無線網路威脅

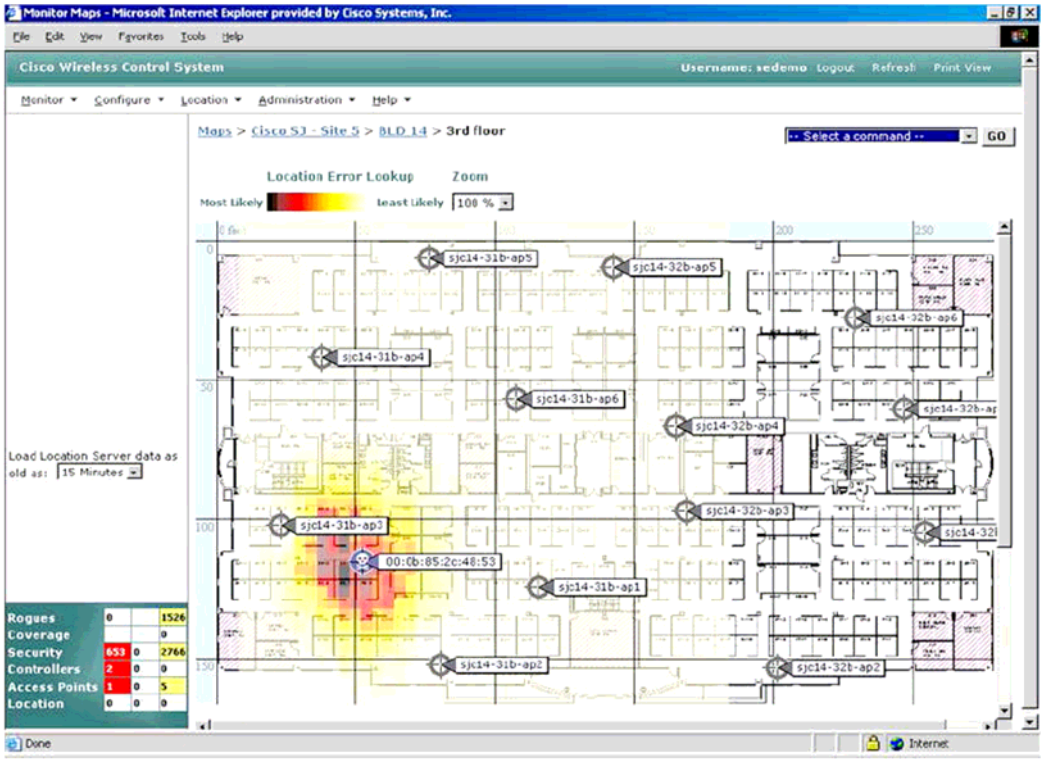
Cisco 統合無線網路整合了無線電資源管理(Radio Resource Management, RRM)以持續監控鄰近的空中區域。嵌入於控制器中的無線電資源管理軟體，作用就像是內建的 RF 工程師，可以持續提供無線網路即時的 RF 管理。無線電資源管理軟體可以讓控制器持續監控相連輕量級 AP 的流量負荷、干擾與其他 AP。當新的控制器與輕量級 AP 加入網路時，無線電資源管理軟體可以自動偵測與並進行設定。

輕量級 AP 可經由設定以偵測所有有效的 802.1a/b/g 通道上的無線網路威脅。這些 AP 以「離開通道」不會超過 60ms 的時間，來監控這些通道。軟體將分析所收集到的封包，以偵測惡意 AP、惡意客戶、特別客戶、與在 2.4GHz 到 5GHz 波段中（例如，藍芽的信號、微波爐烤箱等等）的 RF 干擾的其他種類。由於如此，無線電資源管理軟體也讓 Cisco 統合無線網路，在頻譜的其中一部分偵測到過多的干擾時，得以透過轉換通道的方式，減緩塞爆 RF 阻絕服務攻擊的效應。依預設值設定，每個 AP 只有 0.2%的時間是離開通道的。這樣的活動是分散在所有的 AP 中加以進行，所以鄰近的 AP 將不會在同一時間掃描，若是如此，則可能會反向影響無線區域網路的服務。如此一來，網路的能見度可以提昇，網管人員也就可以看到每台 AP。

## 偵測與防禦惡意 AP 與客戶

不論是服務客戶或是當成空中監控器， Cisco 統合無線網路輕量級 AP 都可以掃描所有 Wi-Fi 的活動。若是一個被管理的 AP 偵測到空中有另一 AP，而且並非由 Cisco 統合無線網路輕量級 AP 控制器所管理，就會將它視為是惡意 AP。惡意 AP 的位置將會在樓層地圖上立即被標示出來（見圖一）。如果經查證後發現是隔壁鄰近的無線區域網路，例如某個上網熱點或是隔壁公司的網路，網管人員可以將其標示為「已知外部惡意」。同樣的，若是內部已知 AP，例如那些在測試環境中的 AP，這些將會被標示為「已知內部惡意」。

圖一 被偵測到的惡意 AP 將被標示在地圖上，以被實體移除




在這個時候，網管人員可以啟動入侵防禦措施。一至四個 Cisco 輕量級 AP，可以防止客戶連上惡意 AP，以進行圍堵動作。這將可以確保從惡意 AP 出來的流量不會進入公司內部網路，直到惡意 AP 被移除為止。

對於沒有網路管理資源的據點，例如分公司或遠距辦公室，能夠自動偵測是否有惡意 AP 連上企業網路，其助益相當大。企業可以採用兩種不同的方法，來判斷是否有惡意 AP 連上企業網路：惡意位置發現協定（Rogue Location Discovery Protocol, RLDP）與惡意探測器。利用惡意位置發現協定，控制器可以指示一個被管理的 AP 連上惡意 AP，並送給控制器一個特別的封包。如果控制器收到該封包，就表示有惡意 AP 連上企業網路。這種偵測方式只對沒有加密的惡意 AP 有效，而大部分員工都是安裝這種消費型等級的 AP。

對擔心有加密的惡意 AP 的企業來說， Cisco 統合無線網路提供一個可以與惡意位置發現協定互補的方法。由於一個有管理 AP 無法連上加密的惡意 AP，所以企業必須採用另外一種方法。在這樣的情境中，當一個客戶連上惡意存取器時， Cisco 統合無線網路將會監控送到網路的位址解析通訊協定(Address Resolution Protocol, ARP)的請求。為了擷取 ARP 請求，可以在每個有線存取虛擬區域網路(VLAN)上的每個網路建置惡意探測器。惡意探測器是無線電被關掉、有管理的 AP，其功能就是探測並儲存所有客戶 ARP 來源 MAC 地址。

當控制器確認惡意 AP 連上一個客戶設備時，它將會要求網路上的惡意探測器去確認是否曾經記錄過該惡意客戶的 ARP。如果 RF 監控 AP 探測到該惡意客戶的來源 MAC，與惡意探測器 AP 探測到的來源 MAC 相符時，就表示該設備已經連上企業網路。

不論是用上述兩種方法的哪一種，如果已經確認惡意 AP 連上企業網路時，惡意警報將會從輕微變成嚴重，網管人員必須立即採取行動以防禦傷害性的活動發生。

## 探測與防禦特殊網路

偵測特殊網路的方式，是透過觀察與分析空中的封包中，那些可以指出該連結為特殊連結或是基礎建設層級的特定訊框。一旦探測到特殊網路，Cisco 統合無線網路可以送給客戶解除連結訊框，以阻止網路連結以防禦傷害發生。

## 探測與防禦客戶錯誤連結

一個結合 Cisco Security Agent 軟體與 Cisco 統合無線網路的統合策略，不光可以探測還能防禦客戶錯誤連結。當客戶連上惡意 AP 時，Cisco 無線控制系統(Cisco Wireless Control System, WCS)將可探測並發出警報，網管人員就可以立即採取行動。然而，利用 Cisco Security Agent 軟體或是第三方客戶防火牆，就可以解除這種特殊的威脅。設定防火牆以同步使用有線與無線介面加以防禦，將可以確保連上企業有線網路的員工，不會一不小心就打開一個通往無線企業網路的橋梁。與單一無線入侵偵測系統相比，Cisco 統合的有線與無線安全策略可以提供更佳的保護。比起僅依賴企業級無線網路 IPS 解決方案，這樣的策略也更為有效，因為當使用者從遠距連上企業網路時(例如從家中或是旅館房間)，也可能出現客戶錯誤連結。

## 探測與防禦阻斷服務攻擊與滲透攻擊

阻斷服務攻擊與滲透攻擊，例如中間人攻擊，乃是依賴愚弄網路訊框，然後再使客戶被取消授權、或是取消結合。Cisco 統合無線網路先進安全服務(Cisco Unified Wireless Network Advanced Security Services)，將建置管理訊框保護(Management Frame Protection, MFP)功能，以探測到被愚弄的單一管理訊框，以確保每天的攻擊保護。MFP 將所有從 AP 到客戶的管理訊框拼湊在一起，然後將這些拼湊訊框，插入附加於訊框上資訊元素(information element, IE)的訊息整合清單(message integrity check, MIC)。只要看到有效的 MIC，有管理的 AP 甚至連單一被欺騙管理訊框都將會被偵測到，並發出新的 IDS 警報。與其他供應商的 IDS 導入服務相比，這是一個非常重要的改善，因為前者通常需要累積相當多的欺騙管理訊框才能發出警訊。

許多供應商為了推銷昂貴、層疊的 IDS 解決方案，用以籠統的方式告訴客戶攻擊發生的次數。然而，無線區域網路滲透訊號的重要性卻遠比偵測惡意或阻斷服務攻擊為低，因為堅強的無線區域網路安全能力，不論是透過 WPA2 或是 WPA，都可以成功阻止任何滲透攻擊。

除此之外，許多 IDS 警報都是虛驚一場，只會浪費網管人員的時間，讓他們追蹤無用的警報。IDS 警報之所以常是虛驚一場，有下列原因：

- **無效安全防禦方法** - 系統建置時並未使用為該工具特別設計的特殊加密與認證方式。舉例來說，當 WEP 不是所使用的安全方法時，為了 AirJack 工具所發出的警報就是假警報。
- **錯誤設定 AP** - Cisco 統合無線網路本身就會根據 WCS 定義的標準模板來設定所有的控制器與 AP，防禦未被批准的安全模式被採用。如果網管人員將 WPA2 或 WPA 定義為標準的安全模式，任何連上網路的輕量級 AP 確定都將使用這個模板。如果 AP 是分開設定(而非集中設定)，人為疏失可能會導致錯誤設定的發生。
- **多變的攻擊方式** - 許多攻擊工具是以開放原始碼為開發基礎，讓駭客很容易巧妙修正攻擊工具以避開 IDS 攻擊辨識特徵偵測。

Cisco 統合無線網路具備無線攻擊辨識特徵的完整資料庫，並可以讓客戶定義自己的辨識特徵。最新威脅資料庫的辨識特徵也會定期更新。然而，這是一個僅能確認威脅的反應方式。因為問題乃在於偵測攻擊辨識特徵的 IDS，Cisco 專注於辨認非法的無線區域網路行為，例如欺騙管理訊框，並非在特定的攻擊辨識特徵上。在大多數的情況下，一旦確認了非法的無線區域網路行為，Cisco 統合無線網路進行防禦並加以阻止，而非只是辨認而已。針對依賴欺騙管理訊框的攻擊，Cisco 致力推動制定加密管理訊框的 IEEE 802.11w 標準流程，帶領業界朝永久防禦機制方向發展。

## 探測偵查檢視

如先前所討論，類似發現網路名稱的 NetStumbler 這樣的偵查檢視攻擊，將不會對擁有適當安全防護的無線區域網路造成威脅。僅是知道網路名稱並不能給駭客任何優勢。Cisco 統合無線網路將會提報類似 NetStumbler 偵查檢視攻擊的出現，然而企業並不用擔心。無線 IDS 供應商將試圖把這種類型的工具，放在他們的攻擊辨識特徵資料庫中，以增加明確攻擊的種類數量。但是最後這些威脅並不會比視窗 XP 自動找到無線網路名稱來的危險。

## 確認無線 IPS 投資的等級

在確認無線 IPS 投資時，企業應該考慮到許多不同的因素。Cisco 建議所有企業都能具備最基本無線 IPS 的能力，以保護公司免受例如惡意 AP 或是阻斷服務攻擊等無線網路威脅。Cisco 統合無線網路整合無線 IPS 的能力，在提供安全防禦時，卻不需增加額外的成本支出。覆疊無線 IPS 供應商經常會強調整合無線 IPS 功能的負面印象，批評這樣的方式並不能提供「持續保護」，因為 AP 同時還需要服務客戶。這樣的說法是錯誤的，因為沒有任何感應器可以一直停留在同一個通道上，不管是專屬的感應器或是一個 AP。所有的感應器都必須不停地在通道間進行切換，以掃描全部的 802.11 信號頻道，偵測威脅。

Cisco 統合無線網路 AP 可以只被當成感應器，跟一個覆疊的無線 IPS 解決方案提供一樣層級的安全保護。事實上，因為整合性解決方案的時間大部分都是應用在使用中的通道上，所以整合無線 IPS 解決方案比起覆疊解決方案，能提供更佳的安全保護來防禦線上攻擊。對照之下，覆疊式解決方案必須在每個通道上耗費相同的時間，因此當攻擊在某通道發生時，它有可能不在那個通道上。

相反的，一個擁有線上無線 IPS 功能的整合性解決方案，具備覆疊無線解決方案所無法提供的獨特好處。只有提供客戶服務的線上系統，才可以認證一個獲授權的客戶。覆疊系統

無法利用空中的交通流量監控來確認客戶是否獲得授權。許多覆疊系統都依賴獲授權 AP 認證的空中探測威脅功能，但是由於覆疊無線 IPS 感應器無法對流量進行解密以確認真實性，所以這個方式並不可靠。一個整合性的解決方案是唯一可以提供阻斷服務攻擊的線上偵測。而一個整合的解決方案甚至還可以將科技升級成本，例如 802.11n，降到最低，原因是只需更換一套系統硬體，而非兩套。最後，整合性的解決方案提供建置、管理與維護行動服務與無線 IPS 的單一平台，降低總體持有成本。

## 總結

想要適當的保護無線區域網路與有線企業網路，網管人員首先應該建置最強大的空中安全系統。只要有可能就應該採用 WPA2 技術，以進行強大的 AES 加密以及網路與客戶間的雙向認證功能。防禦無線網路威脅的第一步，就是必須正面認證授權客戶與基礎建設。除此之外，它還會讓類似 NetStumbler 的偵查攻擊無效：因為當強大的認證功能與加密技術都到位時，就能夠瞭解 SSID 並無用武之地。

一旦授權網路元件的適當認證都到位時， Cisco 統合無線網路可以使用嵌入在每個控制器中的無線電資源管理(RRM)軟體，來分析無線傳輸的封包，並警告網管人員不同種類的威脅，包括惡意 AP、惡意客戶、特殊網路、與阻斷服務攻擊等。RRM 還可讓 Cisco 統合無線網路避免 RF 的干擾。WCS 也可以進行精確的威脅位置確認。網管人員可以採用任何無線的圍堵方法，來解決惡意 AP、客戶或是特殊網路問題。可以透過惡意位置發現協定與惡意探測器等兩種方式來清楚確認惡意 AP 是否連上企業網路。

整體來說，Cisco 的策略是主動防禦威脅，而非僅對其做出回應而已。Cisco 提供無線攻擊辨識特徵的資料庫，但是許多攻擊工具卻可以修改攻擊的辨識特徵。雖然 Cisco 統合無線網路可以讓客戶自訂攻擊辨識特徵，Cisco 卻認為更有效地利用 IT 資源才是永續的解決方案。因此，Cisco 透過在 IEEE 802.11w 標準制訂組織裡的重要角色，正在引導業界除了偵測外，更因向防禦阻斷服務攻擊與滲透的方向發展。目前管理訊框保護功能的準標準版本已經上市。

Cisco 統合無線網路提供許多不同的 IPS 建置模式，可以滿足企業不同的需求。AP 可以用來服務客戶並掃描無線網路威脅，或僅進行空中監控而已。後者功能特別適用於分支辦公室，或是企業總部沒有無線區域網路覆蓋的角落，保護這些地方免於無線網路威脅。跟許多其他覆疊無線 IPS 系統不同的地方是，這種空中監控器之後能被轉成 AP 使用，大幅降低總體持有成本。

**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.**