Extreme™
Customer-Driven Networking

Data Sheet

重點提要

- 24 小時全年無休的 WLAN 網路監控，達到完全阻絕各種無線攻擊活動的效果
- 領先業界的威脅偵測資料庫
- 將感測器資料進行集中彙整與關聯處理，有效減少誤判情況
- 支援大型布署情境下，多台裝置的集中管理
- 藉由自動終止惡意非法行為達到即時偵測惡意非法裝置的效果以快速回應攻擊行為，在裝置可實際移除前持續保護您的網路安全
- 運用平面圖找到惡意非法裝置
- 運用即時通知功能強化政策（Policy）的施行，並依據政策（Policy）違規模式做出適當的回應
- 匿名行為偵測功能可監控無線流量，達到早期預警的目的
- Liveview 提供 25 種以上的圖形化摘要說明、封包擷取與解碼功能，以利分析運作中網路與即時流量

  藍芽監控功能可偵測非預期存在的 BT 2.0 裝置，並依據 BLE 4.0 標籤識別潛在的網路釣魚攻擊行為

Extreme 無線入侵防禦系統虛擬機版

產品總覽

儘管無線連線能力讓企業得以透過威力強大的嶄新方式進行溝通，但也伴隨著各種安全漏洞、操作複雜性與管理問題。若要享有無線網路帶來的種種好處，但又想避免使用者及企業陷入各種安全風險之中，您需要適當的工具組合。

Extreme 無線入侵防禦系統讓您的無線網路安全、監控作業與法規遵循作業更加簡化。Extreme 無線入侵防禦系統以 24 小時全年無休的安全保障持續保護您的網路免於外部威脅，在發生攻擊時通知 IT 人員即時回應。

無線入侵偵測

要讓您的無線資產價值發揮到極致，就必須盡可能將安全防禦工事做到滴水不漏安全性與法規遵循功能能在您的無線網路裡合作無間，共同偵測並消弭各種惡意非法裝置、強化政策（Policy）施行、防止惡意入侵行為，並確保法規遵循。有了自動化威脅消除與政策（Policy）施行工具，您就能自信地即時回應各種威脅，讓效果出色的安全防禦工事帶給您一夜好眠。

Wireless IPS 模組能夠依據歷史資料即時分析現有與零時差威脅攻擊行為，準確地偵測各種無線漏洞與不尋常的網路活動。內容感知式偵測、關聯與多面向偵測引擎能夠有效減少誤判的警報次數。內容豐富完整的威脅資料庫搭配可自訂原則的設定功能，讓系統得以自動回應各種無線安全威脅，有效減少網路所面臨的安全風險。

惡意非法行為偵測與消弭

Extreme 無線入侵防禦系統同時支援專屬（一對一），以及射頻共享（一對多）的作業模式。在專屬作業模式中，額外的基地台將作為專屬的感測器使用，負責 24 小時全天候掃描。在射頻共享模式下，基地台主要負責傳輸資料並定期切換到其他頻道以監控威脅。在此模式下，基地台除了執行感測作業外，還能幫忙基礎架構頻道傳輸資料。專屬的感測功能則可讓無線電波更加透明。透過感測到的資料與延伸關聯功能，此系統可揪出與有線網路連結的真正惡意非法裝置，並將之與鄰近的基地台隔離，進而有效防止誤判情況出現。找到真正的惡意非法裝置之後，系統能夠使用多種不同的技巧執行惡意非法抑制作為，包括無線終止、定位與停用乙太網路交換器上惡意非法裝置接入的連接埠或是使用 ACL 來達到相同目的。

安全性政策（Policy）管理

Extreme 無線入侵防禦系統能讓系統管理員定義需要在網路上施行的各項安全性政策（Policy）。當系統偵測到政策（Policy）違規行為時，就會產生警報。此系統內建警報動作管理程式，經過設定後可以依據警報觸發指定的動作，包括傳送電子郵件給系統管理員、產生系統日誌（syslog）或 SNMP Trap、初始化自動遠端封包擷取，乃至於啟動頻譜分析等。

定位惡意非法裝置

Extreme 無線入侵防禦系統感測器可以定位惡意非法基地台位置與用戶端，並在平面圖上指出其位置。IT 人員可藉此找到這些惡意非法裝置並加以中斷連線。

報告與法規遵循

Extreme 無線入侵防禦系統在網路安全性與原則法規遵循上，內建了一系列報告功能。AirDefense 不但在安全性、基礎架構、裝置清查、法規遵循等功能上提供了多個內建的報告，還提供報告產生器方便系統管理員從資料庫提供的欄位裡進行選擇，以建立自訂報告。自訂報告日後可以用於預先定義報告之類的活動。

Liveview

Extreme 無線入侵防禦系統的 Liveview 模組內建一套工具，能讓您針對無線流量進行即時分析。系統管理員可透過 Liveview 將感測器轉換為網路監聽器，擷取無線電波上完整的第 2 層框架封包。所擷取的封包可以細分為個別欄位以便在 Liveview UI 上進行檢視，或是儲存為 pcap 檔案以便匯入其他封包分析工具（例如，Wireshark）。遠端封包擷取活動，最多可同時由 5 部感測器進行。

除了這項功能之外，Liveview 還提供超過 25 項摘要視覺化功能，能夠將上述擷取的資料化為具體意象以利進行資料分析、裝置分析、連線分析、框架分析等，威力之強大遠遠超出遠端封包擷取功能。

一言以蔽之，Liveview 提供可集中管理的遠端故障排除與資料分析等出色功能，不但有助於從中揪出問題，還能免除派遣技術人員到現場排除問題所需花費的高昂作業成本。

藍牙監控

Extreme 無線入侵防禦系統可以主動監控藍牙裝置。具備藍牙硬體的基地台機型可適用此功能。此功能可用於偵測嘗試開啟網路漏洞的藍牙掃描器（skimmer），以免其運用藍牙通訊協定允許未經授權的存取行為。此外，還可偵聽 Google Eddystone 裡的 URL / UUID 廣告，或是使用 BLE 4.0 通訊協定的 Apple iBeacon 標籤。此功能有助於偵測能夠放送未經授權 URL 的標籤，而這些標籤則可能大開網路釣魚攻擊的方便之門。您可以設定允許清單篩選允許的 URL（例如，內含組織專屬的網域名稱），同時針對可能未經授權的 URL 觸發警示。