PRODUCT DATASHEET

ForeScout™

CounterACT™

Clientless 網路行為安全&隔離控管解決方案

"CounterACT is easy to deploy because it is clientless, it interrogates every single device that touches the network, and it doesn't disrupt our business."

Kenneth Corriveau, CIO, Omnicom Media Group

CounterACT ~ Clientless 網路行為安全 & 隔離控管解決方案

CounterACT 提供獨特的 clientless 網路存取控制（NAC）和 Signatureless 入侵偵測（IPS）功能，保障企業各式資訊設備安全的網路連線政策，同時免於惡意程式（worms, malware）和變種病毒的攻擊。CounterACT 不需更換或提昇網路設備（FW, VPN, Switch），可無縫地與企業現有的環境結合，立即阻斷不信任的設備，保障企業資訊環境的持續運作，為 NAC Solution 的最佳選擇。

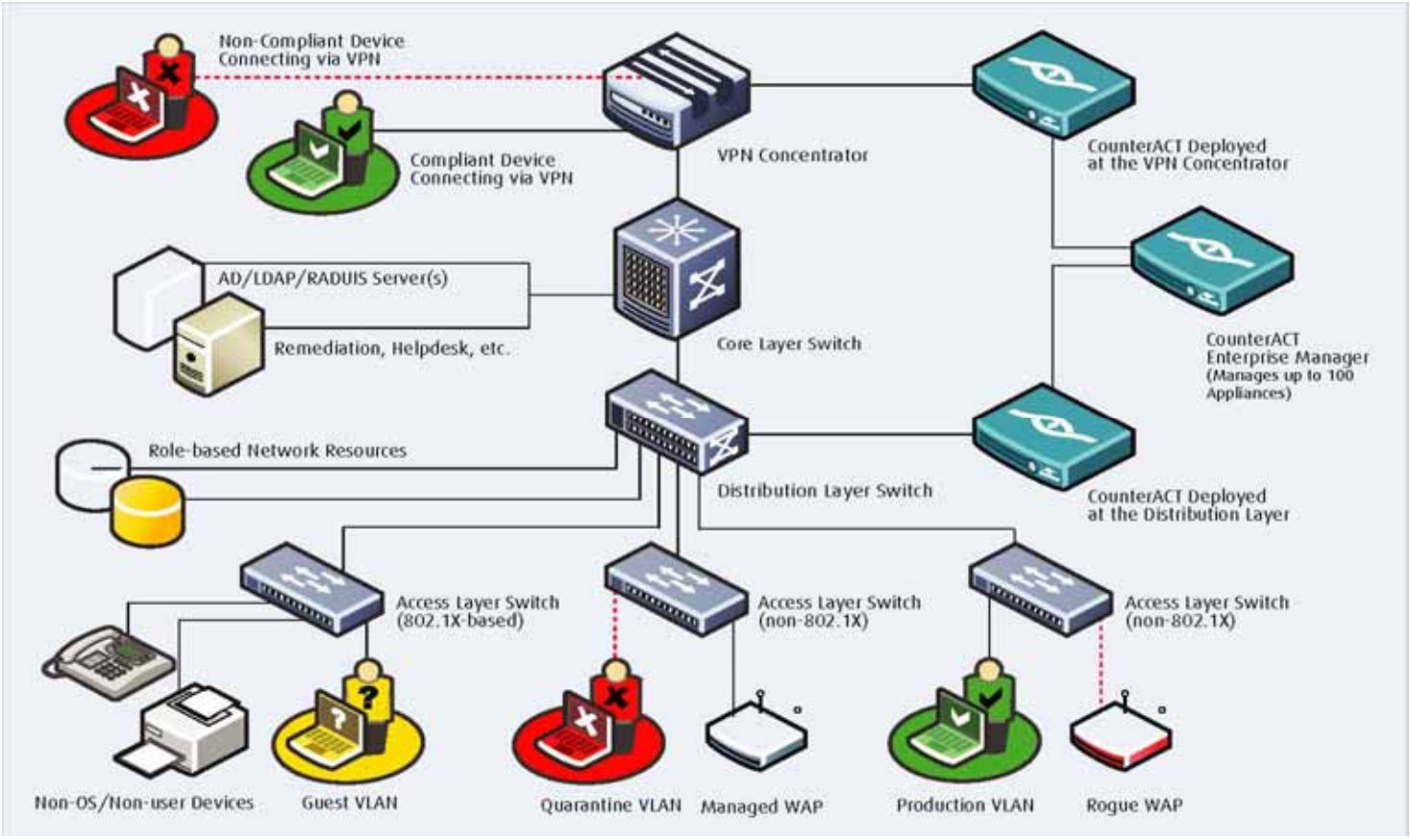
CounterACT 解決了企業網路管制上複雜的問題：各式不同的資訊設備即時的漏洞修補（微軟補丁，病毒碼更新…）、未授權的程式和惡意程式等。運用自動偵測(X-Ray ™)和立即阻斷威脅（擴散式的蠕蟲病毒）之技術，在不改變使用者習慣的前提下，CounterACT 只允許授權的使用者，使用正確的設備連接上企業的網路環境。

現今的企業，面對愈來愈多方面的安全威脅，例如：外聘人員設備造成的安全漏洞，訪客或在家工作的員工避開實體安全的限制，及傳統網路架構無法防制不信任的設備連上網路…等。而 CounterACT 提供不需要安裝 agent 軟體之強制控制網路存取的功能，來防制未授權的資訊設備：如 Desktops, Laptops & non-OS Devices(如：VOIP phones, 手持式設備和網路印表機…等)。

CounterACT 運作方式

CounterACT 採取多種的偵測技術，聆聽網路的流量，可即刻發現新增加的設備，並依據企業訂定的安全政策，以決定此設備的權限是授權用戶（員工），還是非授權用戶（訪客, 聘雇人員 or an unauthorized user）；同時，立即掃描此設備是否帶有蠕蟲或惡意程式，以阻斷其引進的威脅事件發生。依照安全政策，任何設備進入時，CounterACT 可以馬上引導訪客或無作業系統（non-OS）設備至適當地網段；而員工設備則可連結至依其授權分類的合法環境上，CounterACT 會一直持續地監控所有資訊設備，一旦發現員工設備有不安全狀況發生（中毒、攻擊事件），則即刻將之隔離。

Figure 1: Example of a typical CounterACT deployment



端點 X 光機（ Endpoint X-Ray™ ）

CounterACT 提供業界最強的端點審查防護功能，能夠確保端點安全政策的強制執行，快速偵測到入侵事件的發生；同時，運用偵測註冊檔(registry)和檔案系統 (file system)的功能，不用安裝 client agent，CounterACT 即可以判定 client 端各種狀況，包括：是否有安裝個人防火牆、作業系統補丁 &病毒碼更新之狀態，以及是否有企業指定的軟體存在於註冊機碼等各種情形，可以說是最完整且操作人性化的解決方案。

NAC Fastpass™

CounterACT 提供彈性的存取控制政策設定，可以滿足各項客戶的需求。運用 NAC Fastpass 的新技術， CounterACT 不像其他 NAC 產品，會產生”連線隔離”（quarantine upon connection）的等待狀態，以其行為分析模式之入侵偵測功能，快速的判別欲連線設備是否含有惡意程式，並引導設備進入符合安全政策的網段。當然，CounterACT 也支援先隔離檢查再放行的需求，這完全取決於客戶的控管原則。

真正地 clientless NAC

CounterACT並不需要安裝client端agent即能完成各式設備連線的檢驗，即能檢測各式的設備，包括：non-user devices such as network printers, rogue and legitimate wireless access points, VoIP phones and PDAs，只要一連上網路，CounterACT立即可判別設備的類別，是否含有入侵威脅，及將之導入適當的網段位址。

客製化的管制原則

CounterACT 支援各種彈性的管制設定，可依設備類別 (IP range, OS ,AD group, switch location...)，設定網路存取政策和管理方式，不同類別之設備 or 不同群祖之人員，其管理政策不同。例1:低風險管制：針對病毒碼過期的使用者，限制其連線範圍，直到其完成病毒碼的更新。例2:高風險管制：未授權的設備，限制其網路連線；中毒的設備，阻斷其服務或實體網路埠等。

非侵入式的部署方式

企業導入 CounterACT時，並不需要作任何架構上的改變或產生網路昇級的費用， CounterACT採用外接端（out of band）的結合方式，可與原企業環境各品牌產品整合，只要在網路主幹（ Distribution layer）上旁聽，即可管制設備的網路存取。這種非同軸（ non-inline）的佈署方式，可避免單點失效 (single point of failure)之重要缺點；同時，不用改變現有基礎架構，也是最經濟的解決方案。當然，也可以在強制執行安全政策前，先只聆聽網路活動，再逐步實行管制措施。

CounterACT也支援 HA和 DR Site 架構，提供持續性且非侵入式佈署方式。

NAC 儀表板

CounterACT 提供一目了然的 NAC 儀表板功能，可顯示整體企業即時(real-time)和趨勢(trade)的 NAC 資訊，包括：NAC 趨勢、矯正趨勢、各組織 NAC 狀況、企業整體 NAC 狀況、訪客數量、入侵事件、矯正事件、監控數量...等。此儀表板的內容是動態的，會自動的更新 CounterACT 監控下的所有狀態。

未授權的管制

針對未授權的設備（ ex：訪客各種不同的設備），CounterACT 並不需要先安裝 client 軟體，可先視同為已知的設備般處理，一旦確認是不明的設備，會立即將其引導至隔離 VLAN 區，並要求檢驗其細部的資訊；完成檢驗後，再自動引導至符合其存取權限的網段。

整合非特徵碼的 IPS（Signatureless IPS）

CounterACT 是業界目前唯一一個整合非特徵碼式 IPS 的 NAC 產品，其最大的好處是，不需要隨時更新特徵資料。 CounterACT 一旦發現有自行擴散式的蠕蟲或病毒來自於某個設備，在未傷害到整個網路前，就會立即將它阻斷。

Figure 2: Tailored enforcement actions to policy violations.

CounterACT 處理方式

告警訊息	存取限制	處理方式
Open Trouble Ticket	以虛擬防火牆(Virtual Firewall)隔離不信任設備	將設備導入適合的 VLAN（合法網域 or 隔離區）
Send Email	導入不同的 VLAN，限制其存取之資源和服務	結合802.1X，阻斷網路存取
SNMP Traps	結合 Switch, firewall 和 Router，限制其存取	依認證原則處理(IP、MAC、AD、802.1x or Guest HTTP)
Syslog	自動將設備導入訪客網域中	關閉 Switch port
HTTP Browser Hijack		中斷不信任的設備
Auditable End-user Acknowledgement		
Automatic or Self-Remediation		
SMS, PatchLink Integrations		

透通式的管制

導入 CounterACT並不會改變使用者的行為，無論是剛連線或已經存在於網路中的使用者，正常的使用者完全感受不到有 NAC的存在，一旦發現有問題時， CounterACT才會採取隔離措施，並主動通知使用者或技術人員，或要求其執行矯正 (remediation)措施；否則，使用者完全不會查覺到 CounterACT的存在。

與 3rd party 整合

CounterACT 可與多種異質產品整合，包括：交換器 (Cisco、Foundry、 3com、 HP ...)、線上支援系統 (e.g., Remedy)、漏洞補丁系統 (e.g., PatchLink)、防火牆 (e.g., Check Point、Cisco、Symantec、Router ACL)、VPN(Cisco VPN、Juniper VPN、Nortel VPN)和弱點掃描系統(e.g.,Qualys)等。同時，也可透過 API 與遠端監控管理系統整合，或是客製化方式與專屬系統整合。

與 802.1X 整合

CounterACT支援與 802.1X的整合，如果沒有 802.1X，CounterACT也可以提供網頁認證畫面，與原網路環境中的認證方式整合 (如：MS AD, LDAP, Radius, Mac address ...等)，並支援分權控管功能，達到完全阻斷不信任設備的需求。

與 VPN 整合

對於透過 VPN連線的使用者，不論其是使用公司設備或是自有設備，只要連線進入公司，都應該受到公司安全政策的檢驗，CounterACT可與 VPN設備整合，阻斷不信任的設備，如同保護LAN的使用者一般，達到強制管制的目的。

管理和報表功能

每個 CounterACT appliance 設備都提供有 Java-based 的管理功能，在多個設備的環境下 (例如： 100 個 appliance)，則提供 CounterACT Enterprise Manager(appliance)以便集中管理分散式的網路安全政策，下達管理規則至各個 NAC 設備，同時，集中收集所有的資料，產生統計報表。

與弱點掃描整合

CounterACT可結合弱點掃瞄功能，可用以發現潛在性的問題，並配合管制措施，阻擋威脅的發生，並告警使用者。

網路設備 Portal

CounterACT 有提供一套很強的搜尋引擎報表工具，可快速查找違反安全政策、惡意程式攻擊等事件，並提供與其相關的使用者(specific user)、設備(devices)及管理者的紀錄等完整的鑑識資料；同時，此 Portal 也提供 GUI 介面，條件式的查找功能，並可顯示所有與此設備相關詳細地活動及事件。

訪客註冊系統

訪客(例如：簽約商、學生、洽公人士...等)欲連接企業網路可由訪客註冊系統來管理，CounterACT 會先阻擋 or 隔離未取得訪客帳號之設備，待其完成訪客系統之註冊程序，系統會自動產生並告知其授權之帳號/密碼，訪客即可以此帳號登入企業網路，但其活動範圍也僅限於 NAC 管理政策允許之範圍;如有違反,即會被告警並且隔離。

資料庫整合(Database Integration Plug-in)模組

提供資料庫整合(Database Integration Plug-in)功能，與後端資料庫連結，可整合客戶端資料庫中的資產設備資料(客戶現有的資產管理系統、 ERP 系統、CMDB、 MDM)、權限管控資料或是(訪客)認證資料，來達到網路管理自動化的管理方式。

以下為安裝ForeScout軟體版本建議之硬體規格，並不是ForeScout License的級距。

Performance Specifications	X-Small	Small	Medium	Large
Devices	Up to 100	Up to 1,000	Up to 5,000	Up to 10,000
Switch/WLAN devices	Up to 4	Up to 20	Up to 100	Up to 200
802.1x Authentications per second	Up to 5	Up to 10	Up to 42 (+2 vCPUs & 4GB Memory)	Up to 86 (+4 vCPUs & 4GB Memory)
Traffic Monitoring + Captive portal HTTP redirects/min	Up to 100 [Mb/s] 16 [KPPS] 5 HTTP redirects/min	Up to 1 [Gb/s] 166 [KPPS] 10 HTTP redirects/min (+2 vCPUs & 4GB Memory)	Up to 3[Gb/s] 750 [KPPS] 50 HTTP redirects/min (+8 vCPUs & 12 GB Memory)	Up to 3 [Gb/s] 750 [KPPS] 88 HTTP redirects/min (+8 vCPUs & 12 GB Memory)
Virtual Machine Specifications	**X-Small**	**Small**	**Medium**	**Large**
vCPUs	4 vCPUs	6 vCPUs	10 vCPUs	14 vCPUs
Memory	8 GB	14 GB	24 GB	32 GB
Minimum Hard Drive Storage	200 GB	200 GB	200 GB	200 GB

Common Criteria

ForeScout
ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA, USA 95134
Toll-Free (US) 1-866-377-8771 Fax 1-408-371-2284

INFO SOURCE
亞太信息股份有限公司
台北市11070基隆路一段163號10F-1
電話:02 3765-2726 傳真:02 3765-2730
網址:http://www.infosource.com.tw