

需求	客戶環境	客戶問題	產品組合	特色	優勢
虛擬化環境-防毒	桌面虛擬化: VMWare View (內含VMWare vShield Endpoint)	全系統掃描造成系統資源爭奪	Deep Security AV	節省安裝傳統防毒軟體耗用ESX host記憶體 簡化防毒管理,無須安裝更新	唯一整合vShield Endpoint API,無須於guest machine安裝防毒agent的煎煮程式防護解決方案
虛擬化環境 安全防護	伺服器虛擬化:VMWare 4.1 (需VMWare vShield)	無法提供虛擬主機間網路流量防護 舊版微軟系統 Windows2000不再提供修補的伺服器	Deep Security FW/IPS	強化VMWare虛擬平台網路安全 提供客製化服務 降低管理及維運負擔	無須安裝agent,即可於VMWare環境提供FW/IPS功能
重要主機 檔案異動稽核	重要主機 (windows主機或Linux主機) 要安裝Agent	重要營運主機檔案變更稽核	Deep Security Agent	主機檔案異動稽核, 提供客製化介面及功能 降低管理及使用負擔	主機檔案異動稽核客製化
網頁伺服器防護	網頁主機(IIS or Apache) 要安裝Agent	網站應用程式防護 網站資料被竊取問題	Deep Security Agent	主機入侵防護功能 Sql injection、XSS 防護 弱點自動檢查建議、虛擬補丁	單一Agent 提供多功能防護(FW入侵,網帳應用程式防護)
中小企業電腦及伺服器防毒	個人電腦 Windows伺服器	無專屬資訊人員 安裝防毒軟體耗用太多系統資源 防毒軟體版本升級	WFBSS	無須獨立防毒主機 無須維護防毒伺服器 集中控管個人電腦與伺服器防毒、防駭 雲端截毒掃描 網頁威脅防護 網站過濾	節省主機及軟體建置成本 無須增加伺服器維護負擔 雲端截毒掃描,耗用較少用戶端電腦資源
資料防外洩需求	及時防護 安裝Agent, 適用400U以下 Windows OS	擔心員工將機密資料任意攜出? 私人隨身碟任意存取公司資料 擔心員工有意無意觸犯相關法規(個資法..) 擔心電子郵件寄出公司機密資料 員工電腦攜出公司後,就無法控管資料使用 公司發生過資料外洩事件 資料外洩但不知道從何外洩? 稽核內部資料使用狀況上的需求?	DLP	內容過濾與即時防護功能 敏感資料探勘 週邊裝置管控 隨身儲存裝置使用管制 資料竊取程式防護功能	使用者特意進入電腦安全模式仍可提供防護 偵測惡意程式竊取 在地化彈性服務 客製化的報表 支援Windows2k 量身訂做使用者客製化條件 專用佈署工具(適用AD及非AD還單一價格,全功能使用)
	監控分析 不需安裝Agent 對外網路頻寬 < 200M	內部資料流向無法掌控 員工私自存放敏感資料在個人電腦 員工私接網路(3G、iphone、WiFi...)存取敏感資料	NDLP	閘道端內容稽核過濾 資料竊取程式防護功能 稽核但不阻擋	不需安裝Agent, 不消耗使用者電腦資源 多個網路協定偵測(SMTP, HTTP..) 不影響使用者作業

法規遵循需求	及時防護 安裝Agent, 適用400U以下 Windows OS 監控分析 不需安裝Agent 對外網路頻寬 < 200M	是否有符合法規(個資法\HIPPA..) 客戶VIP資料被任易攜出 存放大量客戶資料 公司員工個人資料保護 擔心惡意程式竊取公司資料	DLP NDLP	內建個資法規稽核範本	降低IT導入負擔
資安健檢、資安預警系統、網路稽核	有Mirror 功能網路設備 適用100U以上	公司常常中毒，卻又不知問題在哪？ IT永遠是等事態嚴重才開始處理，無法主動發現問題 買了防毒軟體，仍無法第一時間找到專業人員來解決問題 公司常常中毒，卻又不知問題在哪 我們有好幾個分公司，但都是各管各的，我要如何才能知道是不是別間分公司導致我這邊的病毒問題？ 新聞一直說台灣是殭屍網路大國，要怎樣才知道我們公司是不是已經被入侵了？ 上班時間是不是有人在使用P2P軟體，導致我們的頻寬不足？ 公司內部會不會有人私下提供未經核准的網路服務？ 環境中是否還有我們所不知道的威脅，誰能幫我找出來？	TMS	偵測在網路流竄的惡意活動 找出非公務相關，濫用企業網路資源的行為 找出未經核可私自架設的網路服務 偵測潛伏在公司內網的僵屍電腦活動 偵測網路弱點攻擊(Worm Downad...) 偵測內部網路P2P行為 主動式報表	與趨勢原廠服務中心整合，協助降低企業IT管理成本 透過系統報表有效掌控內部網路安全狀態 提供專殺清毒工具，迅速撲滅有害主機上的惡意程式 可整合網路存取控制(NAC)系統，對於有害主機進行攔截
電腦、伺服器防毒	Windwos、Linux	電腦裝防毒軟體，速度變慢 USB 病毒一再感染 病毒變化很快，有沒有更好的防禦方式 病毒再公司內部感染擴散，一台一台解太麻煩了 防毒軟體抓不到病毒，讓病毒一直感染 看個網頁就感染病毒，很困擾 沒有經銷商協助	OSCE	雲端劫毒服務 網頁信譽評分機制 檔案信譽評分機制 USB 隨身碟控管 企業級集中控管管理 主機資安防毒及防入侵	最完整有效率的雲端安全防護 用戶端網頁保全 提供唯一在地化最優質的原廠後勤支援服務 延伸安全防禦邊界
Apple Mac 電腦防毒	Mac OS	Mac 電腦沒有病毒防護	OSCE+PLM Mac	惡意程式防護	整合現有PC 防毒的管理，不增加管理負擔
Thin client 防毒、	Citrix XenDesktop VDI、 Vmware VMviewVDI	Thin client 環境如果裝防毒軟體，電腦速度嚴重受影響，所以都把防毒移除	OSCE+PLM VDI	自動分配系統資源，防止因掃毒影響主機效能	節省虛擬主機資源

Thin client 防毒 虛擬桌面防毒		一台電腦中毒,全部的現上電腦都會跳警告訊息,很難看 掃描病毒時會造成所有電腦速度變		預先掃描 Golden image 基礎映像檔,減少主機系統負荷 雲端劫毒技術	增加Thin client 用戶端容量
HTTP/FTP 閘道防毒	效能與硬體資源(CPU 記憶體)相關	擔心有問題的電腦上網下載病毒影響內部 有些網頁帶有惡意導引,讓電腦感染病毒 上班時間員工瀏覽非公務相關網站,耗用頻寬,影響工作(股票、Facebook) 無法管理員工上網行為 員工私用MSN/IM軟體	IWSVA	掃描、清除及隔離網頁惡意程式 攔阻有害的惡意網址,增進資訊安全度 提供網站分類過濾功能,增加員工生產力 可自訂網站類別 管理內部員工上網情況 內建記錄檔及管理報表	結合趨勢科技SPN雲端防護技術 多種佈署模式,並可支援HA網路架構