tenable®
network security

Tenable提供持續的網路監測技術，找出安全漏洞、降低風險，確保遵循法規

SCCV結合主動式弱點掃描、法規遵循驗證、封包深度解析和日誌分析，構成即時監控與事件回應平台，將組織的資訊安全風險可視化，加速資安事件回應

全球已經有超過2萬個企業採用Nessus進行弱點掃描與安全稽核，迄今沒有其他公司能像Tenable能如此專注的提供包括作業系統、應用程式、惡意軟體、防火牆、網路設備和行動裝置的風險管理

DATA SHEET

SecurityCenter™ CV continuous view | 安全管理平台

讓你徹底了解你的 IT 環境

SecurityCenter™ Continuous View (SCCV) 將即時的網路封包檢測、日誌分析與弱點管理相互結合，讓企業可以即時持續地監控威脅和違規行為。SCCV安全管理平台，可辨識企業內全部的IT資產、即時檢測系統弱點、持續監控影響企業安全的變更，讓企業全盤了解存在的安全風險，持續監控系統的變化。它還整合了現有網路、安全性和修復系統，提供最新的弱點分析和即時更新訊息，讓企業資訊與稽核人員能做出最快與正確的決定。

使用SCCV您可以：

- 消除風險，不僅在有線或無線網路環境，即使是在智慧手機、虛擬平台或是雲端架構中，仍能持續監控
- 迅速對APT、Botnet攻擊和違反企業資訊安全的行為作出回應
- 找出已被惡意程式入侵的系統
- 簡化資安鑑識程序
- 識別資訊安全風險

主要效益

- 辨識全部 IT 資產，可偵測包含行動裝置等等連線到網路的所有系統、尋找複雜網路區段內不可掃描的資產，並自動評估風險以判定對應的工作。
- 經由統計分析追蹤殭屍網路、蠕蟲、惡意程式和未經授權的系統變更，並從網際網路身分識別、全球威脅資料庫及被攻擊指標等威脅清單中判斷異常狀況，達到即時異常活動偵測。
- 透過分析所有使用者、系統設定、資產及認證資料，並以網路裝置、系統及應用程式的稽核記錄，偵測隱藏的攻擊者、惡意軟體及造成危害的系統，讓企業可以加速事件回應。
- 提供進階分析以及資料相互關聯技術，內置多種可客製化報告，協助您識別和回應安全與法規遵循的問題。
- 主動監控違反企業規範情事，可在遇到偏差狀況時發出警示，並持續追蹤是否符合法規要求，以供稽核。
- 執行稽核與法規遵循報告，依據業界標準及法規授權範圍，例如FISMA、PCI DSS、HIPAA/HITECH、DHS CDM 及 DISA STIG，落實以結果為導向並兼顧安全性與合規性的安全性措施。
- 依照不同角色層級制訂報告、警示和動作，企業可依照自有組織架構制訂和發佈安全報告。
- 結合企業既有資訊安全，網路設備和系統等資訊，透過Tenable強大的自動關聯與分析技術，為企業提供即時的安全管理平台，找出企業內主要的安全風險，準確反應資安事件。
- 有效監控APT(進階持續威脅)攻擊，提供即時分析，協助企業阻絕攻擊。

SecurityCenter™ CV 結合弱點掃描、網路封包監控和日誌分析系統，建構獨特、即時且持續的安全監控平台

管理企業資訊風險的程序，既複雜又零散，尤其是在現今的企業網路上更是難上加難。Tenable SCCV的集中式解決方案中囊括了多種功能，能進行混合式IPv4/IPv6資產探索、弱點偵測與系統設定稽核。SecurityCenter具備可自訂的儀表板、報告、進階資產探索，以及支援企業上下各種角色的報告共用功能，方便您輕鬆監控、分析及交流資訊安全訊息。

全方位的解決方案

SCCV建立的集中式企業安全監控平台，運用了下列的解決方案來整合資料：

- **Nessus®**：全球最為廣為人知的弱點掃描系統，可對網路、手持裝置、系統、資料及應用程式進行深入的掃描作業。
- **Passive Vulnerability Scanner™**：PVS被動式安全掃描經由非侵入性的封包深度檢測 技術，提供即時的網路行為分析和持續性的網路安全評估，成功的消除定期主動式弱點掃描缺點。可即時監控網路通訊，以偵測新的主機、服務、通訊協定及應用程式是否符合企業的資訊安全政策。
- **Log Correlation Engine™**：LCE日誌關聯引擎可以從使用者活動、網路封包、資安設備和主機等目標收集和彙總資料，藉此分析出存在的威脅與合規問題。 匯集和分析來自來自任何應用程式、網路設備、系統或其他 IT 設備的安全訊息和事件解決方案。LCE從syslog、Windows event、Netflow和直接的網路監控中找出異常或惡意活動。LCE可以幫助企業減少時間和精力去執行諸如日誌分析、IT故障排除和安全監控工作。

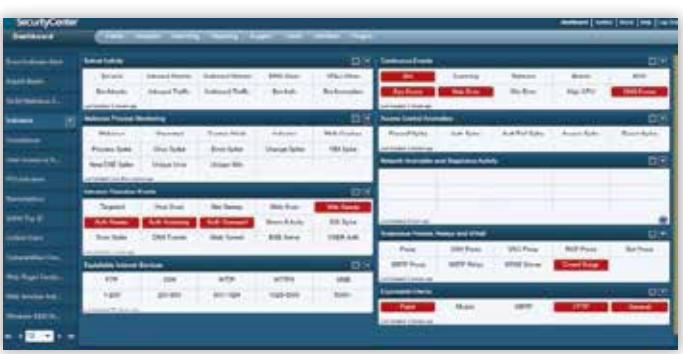
SecurityCenter™ 版本

SecurityCenter™(SC)

對已經使用多個Nessus做週期性弱點掃描的企業，SecurityCenter™提供集中式的管理平台，使得管理人員能讓Nessus掃描更有效率，SecurityCenter能夠連接並管理多個Nessus掃描系統傳來的弱點資訊並整合，讓您一目瞭然，得知企業面臨哪些威脅與風險，還能讓您從單一位置管理弱點資料庫的更新。

SecurityCenter™ Continuous View(SCCV)

SCCV 獨家合併弱點掃描、網路封包檢測、安全資訊及事件管理 (SIEM)，可持續提供精準並能採取行動的安全性訊息。 透過單一系統達成資產探索、弱點掃描、設定檔稽核、法規遵循、網路封包檢測、日誌事件分析、風險報表、告警和工單的統一風險管理平台。



Nessus® vulnerability scanner | 世上最被信賴的弱點掃描工具

產品概觀

Nessus®為業界部署最廣泛的弱點掃描、系統設定與法規遵循驗證產品。Nessus可以進行高速探索、系統設定稽核、資產剖析、敏感性資料探索、修補程式管理整合和弱點分析。Tenable的弱點研究團隊準確的依據環境需求，提供不斷更新的資料庫(plugins)，目前已支援超過65,000個弱點和系統設定檢查。Nessus能擴展並適用於最大型的企業環境，而且部署十分容易。

Nessus 功能特色

- 精確且高速的 IT 資產探索
- 法規稽核：FFIEC、FISMA、CyberScope Reporting Protocol、GLBA、HIPAA/HITECH、NERC、PCI、SCAP、SOX
- 系統設定稽核：CERT、CIS、COBIT/ITIL、DISA STIG、FDCC、IBM iSeries、ISO、NIST、NSA
- 修補程式稽核：包括與 IBM® TEM for Patch Management、Microsoft® SCCM 和 WSUS、 Red Hat® Network Satellite Server 以及 VMware® Go 整合的修補程式管理
- 工業控制系統稽核：SCADA 系統、裝置和應用程式
- 敏感性資料稽核：信用卡資料、個人資訊 (身份證號碼、電話號碼…等) 和智慧產權資料
- 行動裝置稽核：可列出 iOS、Android™ 和 Windows Phone 等連網行動裝置並且偵測出行動裝置的弱點
- 針對以下項目的弱點掃描：
  - 網路裝置：Juniper、Cisco、Palo Alto Networks、防火牆、印表機等
  - 虛擬平台：VMware ESX、ESXi、vSphere、vCenter
  - 作業系統：Windows、Mac、Linux、Solaris、BSD、Cisco iOS、IBM iSeries
  - 資料庫：Oracle、SQL Server、MySQL、DB2、Informix/DRDA、PostgreSQL
  - Web應用程式：Web伺服器、網路服務、OWASP漏洞
  - 入侵偵測：病毒、惡意軟體、後門程式與受到殭屍網路感染之系統通訊的主機、連結至惡意內容的網路服務
  - IPv4/IPv6混合式網路

Nessus 部署方式

Nessus是以設備來做軟體授權，安裝 Nessus scanner的主機需要擁有有效的授權，其中包括：支持無限 IP 掃描內部和外部 IP 地址，可以訪問所有的弱點資料庫和稽核政策，免費的弱點更新和技術支援。

Nessus Cloud結合Tenable PCI掃描服務：Nessus Cloud是Tenable的專業人員，以服務的方式提供客戶針對Internet IP和 web 應用程式進行弱點掃描的稽核，並驗證 PCI DSS的合規事項。
Nessus Cloud以客戶IP為授權，提供服務，包括：Internet IP掃描、PCI DSS稽核服務、弱點資料庫的更新和技術支援服務。

Nessus 稽核方案

Tenable提供Nessus訓練與認證給使用 Nessus 的使用者，協助他們熟悉並且將Nessus效益發揮到最大。Tenable集合多項Nessus稽核人員方案，其內容結合Nessus Cloud、Nessus或上述兩項，搭配Nessus網上課程與認證考試。

全球已超過2萬個企業使用，在資訊安全和法規遵循產品中，獲得眾多專業人士認可

產品效益

- 輕易客製化以達到企業不同的需求
  - 彈性部署、掃描和報告
  - Nessus 可透過電子郵件通知掃描結果、弱點修復建議
  - 弱點修改
- 迅速且全面性的安全評估
  - Nessus可整合修補程式管理系統(patch management systems)更清楚且有效的識別系統狀態
  - 提供尚未安裝的修補程式清單
- 有效降低網路威脅、弱點、合規和稽核風險
  - 掃瞄後以附件方式自動寄出分析結果
- 低建置成本
  - Nessus包括了軟體更新、合規和稽核檔案的線上下載並且享有原廠技術服務
  - 自動的弱點資料庫更新
- 可利用瀏覽器隨時隨地連接到Nessus
- 高度精確的掃描和極低的誤報率
- 最完整的掃描能力和功能
- 易於部屬和維護

部署和管理

- 彈性靈活的部署：可透過軟體、硬體、虛擬平台或以服務方式部署
- 不需要安裝代理程式，容易部署和維護
- 以瀏覽器就能完成的安裝精靈
- 透過 Nessus 的介面進行設定和管理
  - 可使用內建掃描範本，或使用眾多外掛程式篩選工具輕鬆建立掃描政策
  - 可設定掃描排程，執行一次性或定期定時掃描
- 依據嚴重性將風險報告區分為五大類別：
  1.重大風險 2.高度風險 3.中度風險 4.低度風險 5.消息性風險

報告和管理

- 靈活的報表制訂：可依弱點、主機名稱等條件自行定義報表，亦可依掃描結果編排自有格式的報告
  - 提供XML、PDF、CSV 及 HTML 報告格式
- 可將掃描結果寄送給指定人員，並提供修復建議及掃描改進方案

Nessus *可透過電子郵件通知掃描結果、弱點修復建議及如何改善未來的掃描。*

PVS passive vulnerability scanner™ | 被動式安全掃描

產品概觀

Passive Vulnerability Scanner™ (PVS)被動式安全掃描是一項已取得專利的網路探索及弱點分析技術，可藉由非侵入性方式，提供持續即時的網路狀態剖析及監控。PVS被動式安全掃描能在網路通訊中監控IPv4與IPv6網路，以判定拓樸結構、網路服務、網路流量和弱點。而整合了PVS被動式安全掃描的Tenable SecurityCenter™，還能集中分析日誌、管理弱點，讓您全面檢視企業的安全情勢。

產品效益

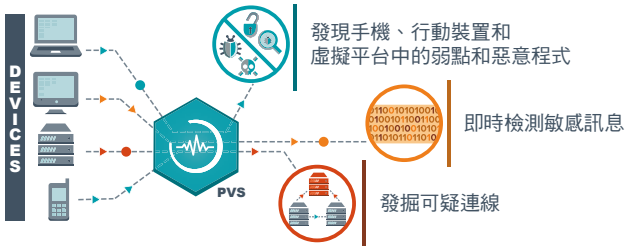
核心及顯著效益包括，可擷取IPv4 / IPv6網路設備、伺服器與應用程式，找出系統弱點和威脅：

- 即時發現威脅，消弭與主動式弱點掃描之間的落差
- 自動找出資產、新系統或惡意系統所帶來的潛在安全威脅
- 透過驗證設定管理，讓企業可確認內部政策及重要法規的合規性
- 可找出可能造成個資外洩的敏感資料
- 可對「真正」的威脅發出警示，讓您專心因應資安事件
- 可找出不當使用的情形及揪出一般設備偵測不到的「內部威脅」
- 可保護因為政策或系統設定而無法進行主動式弱點掃描的系統與應用程式
- 無需登入系統即可執行高效率的掃描，且不會影響服務及不會造成服務中斷

功能特色

PVS 被動式安全掃描可持續監控網路通訊中各種安全相關資訊，包括：

- 追蹤所有客戶端、伺服器和應用程式弱點
- 第一時間確認應用程式是否因遭攻擊而造成資訊外洩或破壞
- 偵測及記錄加入網路的新主機
- 即時發現是否有系統開始對其他系統進行通訊埠掃描
- 顯示所有連線及加密的網路通訊
- 找出個別系統運作的通訊埠以及瀏覽過的通訊埠
- 被動式確認各個運作中主機的作業系統
- 偵測網路上的弱點，以及所使用的通訊協定與應用程式
- 準確偵測APT 、Botnet攻擊



持續不間斷地監控網路流量，找出未經授權的裝置、弱點及混合在IPv4/IPv6網路中的殭屍網路

PVS被動式安全掃描採用非侵入性方式，持續掃描及評估組織的安全性，將組織的安全威脅可視化、數據化。PVS被動式安全掃描能監控網路通訊以判定網路拓樸、讓您深入檢視伺服器與用戶端的弱點、監測網路環境中的敏感性資訊及常見通訊協定與服務的使用情況(例如：HTTP、SQL、共享檔案...等)。PVS被動式安全掃描甚至可在混合式網路中找出IPv4與IPv6 資產。

PVS被動式安全掃描完善的介面與安裝精靈，能讓您毫不費力快速地安裝在網路上，它能被動式偵測網路上的設備(包括行動裝置)，連有越獄(Jailbroken)的iOS裝置都找得到。PVS被動式安全掃描可偵測作業系統、服務、應用程式及所有網路通訊中的弱點問題，有效識別行動裝置的應用程式與弱點。

PVS被動式安全掃描可連接一到多個網段，持續監控網路資料流，發出即時警示，並產生綜合性報告供安全團隊、IT 團隊及管理團隊參考。

網路與 FTP 監控

PVS被動式安全掃描可直接分析封包資料流，擴大監控網路與FTP活動。它能藉著被動式監控所有HTTP或FTP封包，對網路上的各個主機做出判定，並產生實用的報告，例如：

- 所有用戶端及伺服器的漏洞及相關的應用程式
- 完整列出每部主機使用的網路代理程式
- 列舉經由 FTP 共享的所有檔案
- 即時記錄 Web Server 所有 GET、POST 或 Download 的檔案
- 即時記錄所有 FTP 檔案 GET 或 PUT
- 即時記錄所有 DNS 查詢數據

這些高實用性資料，能有效分析內部活動、員工活動以及惡意程式感染或進階持續性滲透攻擊(APT)。大部份這類記錄也能傳送至Tenable Log Correlation Engine™日誌關聯引擎，做進一步分析、搜尋相互關聯性及長期儲存。

不需在伺服器上安裝代理程式也不需要登入到伺服器

PVS 被動式安全掃描可提供Microsoft SMB通訊協定的進階通訊協定分析。如果將PVS被動式安全掃描部署在內部網路，系統就能查看Active Directory 網路流量，並自動學習：

- 各個系統的主機名稱與工作群組名稱
- 所有資料夾中全部共用檔案的清單
- 即時登入資訊和從網路共享下載的檔案

以上被動式判定資訊的能力，給予企業在法律舉證方面極高的價值。在大型網路上，若能判定所有共用資料夾內容，那麼要找出潛在敏感資料就不再是難事。只要將網路上共用的各個檔案記錄傳送至Tenable Log Correlation Engine日誌關聯引擎，即可分析員工活動與惡意程式活動是否合法。

SQL 資料庫記錄與監控

PVS被動式安全掃描也能透過網路通訊內容識別SQL資料庫及與其相關聯的弱點，並即時記錄活動。PVS被動式安全掃描將SQL資料庫查詢的即時記錄傳送至Log Correlation Engine日誌關聯引擎，便能為您搜尋、儲存、關聯及分析攻擊事件，例如來自網路服務的SQL Injection（SQL資料隱碼攻擊）。而利用PVS被動式安全掃描，Nessus SQL掃描及審查 LCE SQL代理程式，企業就能全面性了解SQL資料庫的活動。

被動式的探索網路拓樸與服務

藉著重新建構來源和目標兩端的網路通訊內容，PVS被動式安全掃描能夠以HTTP、SMTP和FTP的通訊特徵去識別它們，並以特定的弱點測試插件去測試弱點。

部署選擇

PVS被動式安全掃描可單獨安裝也可搭配 SecurityCenter Continuous View (SCCV)使用。相當適合持續監控小型網路區段或大型網路中特定網段；而PVS被動式安全掃描單機版提供的整合式介面，能輕鬆監控高敏感性的網路或網路區段，準確點無與倫比。SCCV是一款安全風險管理解決方案，能以獨一無二的方式結合了主動式弱點掃描、被動式安全掃描和即時事件回應平台。

LCE log correlation engine™ | 日誌關聯引擎

產品概觀

Log Correlation Engine™(LCE)日誌關聯引擎，能針對網路和系統中的事件做日誌分析，例如來自原始網路通訊、入侵偵測及永久儲存系統、防火牆、伺服器、應用程式與使用者活動...等等，進行彙總、正規化、相互關聯和分析。透過自身的動態負載平衡機制，能讓多部LCE日誌關聯引擎一同運作，由Tenable SecurityCenter™平台進行事件與日誌分析。

產品效益

- 可藉由單一的管理平台，對企業內任何設備或應用程式產生的日誌資料，進行正規化、相互關聯及分析，藉此瞭解使用者與網路活動，最佳化資訊安全管理與運作
- 可儲存、壓縮及全文搜尋上千部網路設備和應用程式產生的任何日誌
- 符合資訊系統稽核功能，透過企業內部政策及要求以達到合規審查
- 可監控檔案及目錄是否有未經授權的變更與刪除
- 當遇到資安事件，搜尋資料能儲存為壓縮格式，並附上檢查碼，讓資料能夠作為法庭上的證據
- 可擷取使用者的存取記錄與行為，進行內部安全威脅剖析，以判斷員工在網路上瀏覽了哪些網站、存取哪些系統和執行哪些程式
- 可將不符合現行規則的所有記錄歸類為「不匹配」，並儲存供進一步分析，以對先前所忽略的網路行為提供進一步的解析資訊
- 全文檢索能更快、更有效的分析和發現攻擊，進而提昇操作效益
- 可監控本機與遠端 Windows 系統 USB、CD-ROM 及 DVD 的活動
- 可自動偵測偏離日常基準活動的所有日誌，包括防火牆日誌的異常變動、網路應用程式錯誤率的異常以甚至發現阻斷服務攻擊DoS(阻斷服務)和APT(進階持續威脅)攻擊
- 可提供報告與評估表給管理人員，持續不間斷地檢測風險與法規遵循

功能特色

日誌集中管理

LCE包括了完整的日誌管理工具，透過獨特技術，LCE收集、正規化、檢索、壓縮和儲存來自企業內如：Firewall、IPS/IDS、Switch、VPN、Access Point、Proxy、Server、Database、防毒軟體、應用程式...等等的日誌。藉由單一的日誌管理平台，企業可將資訊匯集在單一平台上進行快速且準確的分類和搜尋。而且LCE還能對收集的日誌作關聯分析，將網路攻擊行為如：Password Crack、DDoS、APT和Botnet行為可視化，對平常容易被忽略的日誌作進一步分析或從當中找出可疑行為。

LCE亦可為系統中的檔案進行監控，當指定的檔案被變更、刪除或新增時(例如：網頁被竄改、重要系統遭受變更)，LCE能立即發現，並自動的透過email、syslog、警示、報表等方式通知管理人員，達到7x24隨時監控的目標。

透過LCE內建的近千種，或企業依需求自訂的儀表板和報表，IT人員能夠輕易的對危害企業的資安事件進行響應，有效解決企業內遭受到的攻擊事件和違規行為。

異常偵測與事件關聯分析

LCE日誌關聯引擎在收集到事件之後，會針對每部裝置作統計剖析，來預期裝置的行為變化。只要偵測到不尋常的活動，就會發出警告，例如事件類型增加、連線增加、用戶端或伺服器行為出現劇烈變化。

LCE日誌關聯引擎囊括了眾多先進的相互關聯規則，可以找出蠕蟲發作、無線網路遭誤用等情形，此外還能將IDS事件相互關聯，偵測洩漏狀況。這些規則都是以Tenable Application Scripting Language (TASL)所編寫，可視需要增補、修改或定義。

效能表現

在每秒超過 30,000 筆事件 (30,000 EPS) 環境中，LCE日誌關聯引擎仍能進行即時正規化，分析及關聯分析。而多數事件搜尋，LCE幾乎是瞬間就能讓網路安全與稽核團隊明察秋毫，令威脅與錯誤設定無所遁形，以找出是否有異常狀況、錯誤、殭屍網路、惡意行為以及不尋常內部活動的跡象。任何經LCE日誌關聯引擎正規化的事件，隨時都可作搜尋與分析。

卓越的安全解決方案供應商，能提供整合為一體的安全及合規監控解決方案

一個企業級安全監控平台，就是Tenable Continuous Monitoring的架構核心。

SecurityCenter Continuous View (SCCV)提供不同角色的登入權限介面，不僅能管理多個Nessus®弱點掃描和LCE日誌關聯引擎，還能相互關聯即時弱點監控、重大日誌/事件監控以及自訂合規監控功能，方便讓使用者評估、交流及報告結果，以便做出有效決策。

SecurityCenter Continuous View (SCCV)可結合弱點掃描、網路流量分析，並整合既有資產及網路管理工具，將IT資產分門別類，然後讓上述所有資訊與全公司的日誌資料相互關聯，提供一個針對系統及網路活動的全面性檢視。

報告與分析

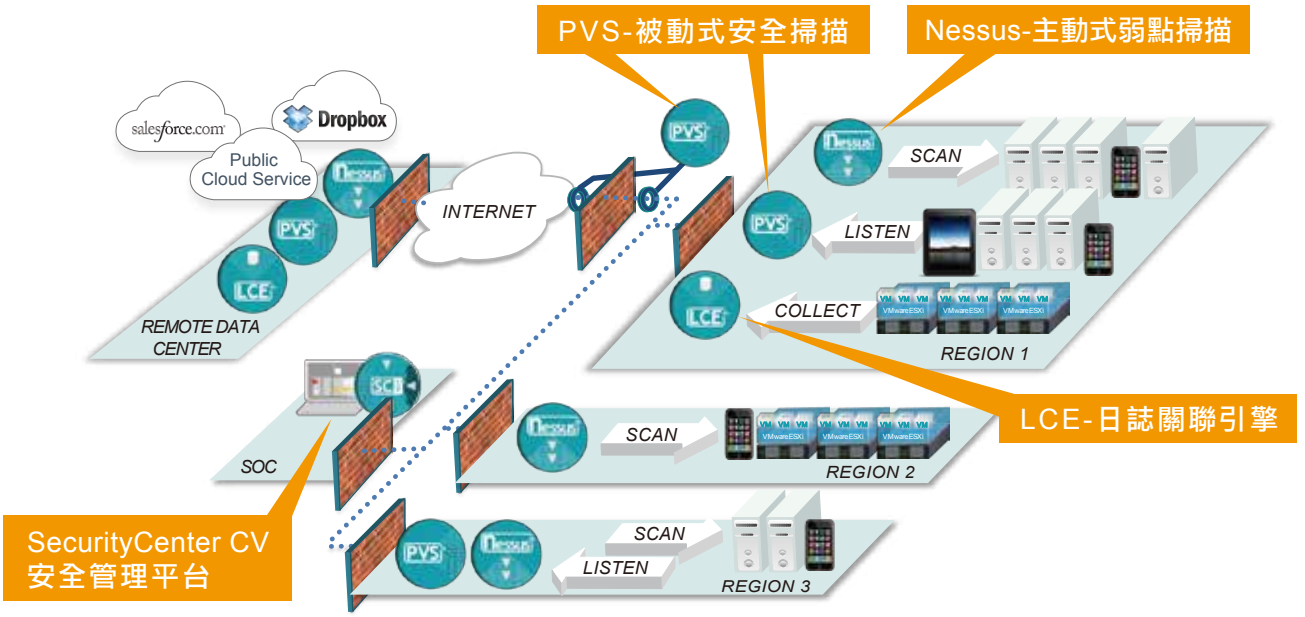
SecurityCenter Continuous View (SCCV)具備分散式管理功能，可從多個LCE日誌關聯引擎資料庫中擷取所有弱點、入侵事件和記錄事件，分毫不差地加以分析和報告，只要一個網路介面就能萬事包辦，包括：

- **日誌保留** – 日誌經傳送至LCE日誌關聯引擎，能儲存於硬碟、轉送至SYSLOG 伺服器或寫入儲存區域網路 (SAN)，以支援法規遵循工作或法律調查程序。LCE日誌關聯引擎上的記錄資料能自動循環和歸檔，並以壓縮格式儲存，方便透過 SecurityCenter 進行搜尋。
- **Log Correlation Engine** – 每個LCE日誌關聯引擎均可連線至數千部LCE用戶端，收集Windows日誌、系統指令、系統記錄、網路通訊以及檔案完整性資訊。

集中式管理

LCE日誌關聯引擎用戶端支援多種集中管理和控制，大幅減少部署及管理時間。實現高部署效率並能即時修改用戶端設定。

SecurityCenter™ CV continuous view | 部署架構



Note:

如需更多資訊

或有其他問題，或有意購買或評估試用，請洽：

UNIFORCE
創泓科技股份有限公司

台灣地區授權代理商
創泓科技股份有限公司
地址:台北市內湖區內湖路一段322號6樓
電話:(02)2658-3077
傳真:(02)2658-3097
客服:0809-085-580
網址:www.uniforcetech.com.tw

tenable network security

For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact