NetIQ Sentinel Log Manager

簡單、符合成本效益的記錄管理部署程序

NetIQ® Sentinel™ Log Manager 是一款全方位的軟體裝置，可讓組織以簡單、符合成本效益的方式，鞏固 IT 企業安全並簡化法規遵循作業。NetIQ Sentinel Log Manager 可降低部署與管理的成本及複雜性，且無需使用昂貴的專屬硬體或大幅變更基礎架構。本產品將記錄管理軟體、內嵌式作業系統及自動更新服務全部納入單一產品，因此您只需要花費幾分鐘時間安裝，即可馬上開始使用產品內建的強大功能。本產品在安裝過程中會自動偵測大部分的資料來源，您只需要微調組態設定。這款新穎的解決方案可讓您運用現有投資，且可在幾乎任何硬體上部署產品，因此能夠大幅降低成本與技術複雜性。

NetIQ Sentinel Log Manager 提供可擴充且符合成本效益的智慧型軟體裝置記錄管理解決方案，供您主動管理風險。其先進、靈活的資料收集與報告功能可讓您全盤掌握 IT 基礎架構的狀況，從而做好風險管理。此外，本產品也能提供達到法令規章要求所需的鑑識證據，並且具備調查回應與主動式安全管理功能，藉以簡化法規遵循的工作。NetIQ Sentinel Log Manager 建置於 NetIQ Sentinel 這套強大、可靠的 NetIQ 安全資訊與事件管理 (SIEM) 解決方案上，讓您部署全方位的軟體裝置記錄管理解決方案，進而迅速獲取投資報酬。

安全且彈性的資料收集

NetIQ Sentinel Log Manager 提供內建的 syslog 支援，並可透過多種通訊協定收集原生記錄。

解決方案
安全管理

產品
NetIQ® Sentinel™ Log Manager

簡化法規遵循作業、改善安全狀態，提供強大的法規遵循與安全防護基礎。

NetIQ

NetIQ Sentinel Log Manager 是一款可立即執行的軟體裝置，結合了 SUSE® Linux Enterprise Server 11 作業系統、NetIQ Sentinel Log Manager 軟體以及更新服務。使用 VMware 或 Xen 將本產品部署為虛擬裝置時，NetIQ 自動更新服務可確保作業系統與軟體隨時都是最新版本，更新作業再輕鬆不過。

本產品除了支援用戶資料訊息包通訊協定 (UDP) 外，還支援透過更安全可靠的傳輸控制通訊協定 (TCP) 及輸送層支援 (TLS) 通訊協定傳送 syslog，這些通訊協定支援驗證和自定證書。NetIQ Sentinel Log Manager 可自動偵測不同的事件來源類型 (例如 PIX、Linux 和 Solaris)，並具備通用 syslog 收集器，可處理無法辨識的 syslog 事件。

NetIQ Sentinel Log Manager 運用備受肯定的 Sentinel 資料收集架構，可為資料庫、作業系統、目錄、防火牆、入侵偵測及預防系統、防毒應用程式、大型主機、Web 伺服器、應用程式伺服器等提供各種資料收集器。這些解譯收集器會進行記錄資料剖析、標準化、過濾和增強，協助事件的分析、視覺化和報告，以達到您的安全性和法規遵循要求。除了這套解決方案內建立即可用的收集器外，您也可以自定或建立您專屬的收集器，以滿足貴組織的獨特需求。

彈性且最佳化的資料儲存方式

專屬的儲存解決方案不但會大幅增加整體成本，同時也會造成對廠商的報告與搜尋工具的依賴。NetIQ Sentinel Log Manager 將收集的記錄資料儲存在標準儲存系統上，並提供資料簽名來確保記錄完整性，因此您再也無須使用昂貴的專屬儲存解決方案。為了將儲存需求降至最低，這套解決方案會自動以 10:1 的比例壓縮資料。NetIQ Sentinel Log Manager 可輕易連線至儲存區域網路 (SAN) 或網路附加儲存 (NAS)，有助您擴充歸檔儲存容量，靈活運用現有的 IT 投資。

彈性的搜尋與儲存功能

分散式搜尋功能可讓您在遠端位置部署解決方案，並從單一主控台搜尋所有的事件資料。此功能可讓您隨手掌握並輕鬆存取事件資訊，進而為稽核做好萬全準備，或簡化遵循政府法規的作業流程。收集的記錄資料保存長達一定的時間後，大多數組織都會將資料歸檔，以便長期儲存。可惜的是，當您需要查詢或報告歸檔的資料時，多數的記錄管理解決方案都會要求您先將資料移回短期儲存空間。NetIQ Sentinel Log Manager 可掛接歸檔資料儲存庫，因此可以查詢和報告本地和歸檔的資料，進而大幅簡化並加速法規遵循作業和鑑識分析程序。

動態的單鍵報告功能

NetIQ Sentinel Log Manager 採用資料索引及單鍵報告方法，能大幅簡化稽核與法規遵循作業的報告產生程序。NetIQ Sentinel Log Manager 可讓您輕鬆、安全地收集和搜尋本地或網路的事件資料，並提供多種內建報告供您選擇，以迅速達到 支付卡產業資料安全標準 (Payment Card Industry Data Security Standard，PCI-DSS)、健康保險及責任法案 (Health Insurance Portability and Accountability Act，HIPAA)、沙賓法案 (Sarbanes-Oxley Act，SOX) 及其他許多法令規章的要求。有了直覺式搜尋和單鍵報告功能，Sentinel Log Manager 這套工具適用於各種需要透明化與記錄分析的情況，例如產生每週必要報告，或在特定安全事件發生後進行詳細的鑑識分析。

使用 NetIQ Sentinel Log Manager 的單鍵報告功能，您不必花費數小時進行自定，也能收到並解譯來自各種不同資料來源的資料。使用以 Lucene 為基礎的強大搜尋引擎，您只需輸入想要報告的準則，NetIQ Sentinel Log Manager 便會傳回一份足以滿足許多基本法規遵循和稽核需求的簡易結果清單。只要按一下滑鼠，就能將這些結果自動格式化為更正式的形式，以最常見的法規遵循及稽核報告所需的特定欄位和參數來顯示結果。您也可以自定或建立您專屬的格式化樣板。

直覺式且操作簡便的介面

NetIQ Sentinel Log Manager 運用 Web 2.0 技術，提供直覺、簡單易用且回應迅速的介面，帶來卓越的使用者體驗。您可以輕鬆透過該介面來檢視資料使用趨勢，並發現潛在問題。該介面也可讓您設定資料收集、進行排程及管理報告、建立資料保留規則，以及設定資料過濾與動作的規則，例如電子郵件警告、傳送簡易網路管理協定 (SNMP) 陷阱、寫入檔案，或甚至將事件轉送至 NetIQ Sentinel 進行即時分析處理ss。

即時 SIEM 的基石

NetIQ Sentinel Log Manager 除了提供快速、簡易的方式來因應您的法規遵循和稽核考量，同時也是導入即時 SIEM 的堅實基礎。大部分的記錄管理產品既不具備完整 SIEM 整合，亦無法提供輕鬆導入完整 SIEM 的途徑。然而，NetIQ Sentinel Log Manager 卻能輕易整合 NetIQ Sentinel 的即時監控功能，以及 NetIQ 的法規遵循管理和身分識別與存取管理解決方案。NetIQ Sentinel Log Manager 提供您一張明確的發展藍圖，讓您逐步導入具備身分識別偵測功能的安全防護，隨著對安全及法規遵循的需求增加，緊密無縫地加入並整合新的功能。

NetIQ Sentinel Log Manager 的主要功能和獨特優勢

- 簡單、符合成本效益的記錄管理部署
  - 提供全方位的軟體裝置記錄管理解決方案
  - 可在 VMware、Xen 或空機上執行
  - 降低部署與管理成本
  - 可擴充式解決方案，提供每秒 500 個事件 (EPS)、2500 EPS 或 7500 EPS

NetIQ Sentinel Log Manager 提供資料索引和單鍵報告功能，能大幅簡化稽核與法規遵循作業的報告產生程序。這套產品也可結合歸檔資料儲存庫，讓您流暢地查詢並報告本地及歸檔的資料，進一步簡化和加速法規遵循作業。

NetIQ

欲進一步瞭解 NetIQ Sentinel Log Manager，或要開始試用，請造訪 **www.netiq.com/sentinel7**。

- 進階且彈性的記錄資料收集功能
  - 運用 NetIQ Sentinel 進階、彈性的記錄資料收集功能，包括內建 syslog 支援，以及從其他協定收集原生記錄的功能
  - 自動偵測記錄來源
  - 支援收集無法辨識的記錄訊息，並進行有限的處理
  - 支援高 EPS 率的資料收集
- 分散式搜尋與單鍵報告功能
  - 從中央主控台流暢地查詢及搜尋歸檔資料與本地資料
  - 使用單鍵報告功能和隨附的報告格式，將搜尋轉換成可重複使用的報告
  - 透過搜尋結果的超連結，快速追溯並細分搜尋準則
  - 提供立即可用的報告和 Ad-hoc 索引搜尋，包括 Ad-hoc 鑑識搜尋
  - 隨附 Web 2.0 搜尋工具，可在找到更多結果時自動更新搜尋結果
- 安全且具成本效益的資料儲存方式
  - 自動壓縮資料，發揮儲存容量的最大效益
  - 使用資料簽名來確保記錄完整性
  - 啟用非專屬本地資料儲存以及 SAN 和 NAS 連接性來擴充歸檔容量
  - 支援可自定的保留規則
- 簡易、可擴充且強大的管理功能
  - 具備直覺式 AJAX 介面
  - 能以圖形顯示資料使用趨勢和任何潛在問題
  - 可輕鬆整合來自 NetIQ 的 NetIQ Sentinel、安全與法規遵循管理，以及 身分識別與存取管理解決方案，進而獲得完整的 SIEM 功能

全球總部
1233 West Loop South, Suite 810
Houston, Texas 77027 USA
全球：+1 713.548.1700
美國/加拿大免付費電話：888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

如需本公司在北美、歐洲、中東、非洲、亞太地區和拉丁美洲辦事處的完整列表，請造訪 **www.netiq.com/contacts**。

追蹤我們的動態：

NetIQ、NetIQ 標誌和 Sentinel 是 NetIQ Corporation 在美國的商標或註冊商標。所有其他公司和產品名稱可能是其各自公司的商標。

© 2012 NetIQ Corporation 及其分支機構。版權所有。

PB595002SLM ENG A4 PO 05/12 F
577-TW1001-002 DS 06/07