# NetIQ Sentinel 7

*簡易又強大的安全管理*

## 簡介

企業組織的 IT 基礎架構及其應用方式，正面臨著大幅度的轉型。這類轉變衍生諸多困難與挑戰，衝擊企業組織保護自身安全的能力。

舉例來說，虛擬化、雲端運算和行動技術，改變了企業組織從事業務活動的方式。這些技術改變了使用者的行為，讓使用者以嶄新、精彩的方式消化資訊，或與他人互動。然而，這些技術卻也造就了分散、互連的企業架構，使得資訊安全管理人員愈來愈難以有效監控和維護企業安全。

為了改善整體的安全狀態、制定更明智的決策，企業組織需要安全事件的即時資訊與分析。他們必須有能力化繁為簡，管理大量的安全資料、處理複雜威脅，並實施不間斷的規則控管。他們需要一套適當的解決方案來協助他們快速、準確地從大量事件資料中，判斷出哪些事件構成重大事件與安全異常狀況。

## 產品綜覽

NetIQ® Sentinel™ 7 能夠讓企業組織即時掌握 IT 活動的全貌，以降低安全威脅、改善安全作業，並在實體、虛擬和雲端環境中，自動實施規則控管。本產品能減少傳統安全性資訊與事件管理 (SIEM) 的複雜性，降低 SIEM 在導入方面的障礙，讓所有企業組織都能輕鬆獲取安全情報。NetIQ Sentinel 7 也將即時情報、異常狀況偵測及使用者活動監控功能結合起來，提供預警機制和更準確的 IT 活動評估，為企業組織帶來一套更有效率的 SIEM 解決方案。

NetIQ Sentinel 7 是業界唯一與身分識別管理系統緊密整合的產品，能將使用者與整個環境中的特定活動相連結。因此，本產品能夠讓企業組織輕易辨識重大風險、大幅加速反應時間，並在威脅和安全漏洞對業務造成影響之前，快速進行矯正。藉由提供即時情報，Sentinel 賦予企業組織防範先進威脅、改善安全作業、持續施行規則控管的能力。

**解決方案**
安全管理

**產品**
NetIQ® Sentinel™ 7

NetIQ

*「即使我們當時每日遭遇高達 35 件嚴重安全事件，Sentinel 讓我們能夠達成早期偵測與快速解決的目標，因此這些事件對於運動賽事的進行並未造成任何影響。」*

**Vladan Todorovic**
Atos Origin 的青年奧林匹克運動會技術與 IT 安全經理

## 功能與特色

- **異常狀況偵測** – 要從眾多事件中，辨識出需要調查的真實或潛在問題，往往是相當困難的。NetIQ Sentinel 的異常狀況偵測功能可自動辨識組織環境中的不一致情形，而無須建立關連規則 (建立關連規則時，您必須明確知道您要找的是什麼)。當您導入 Sentinel 時，您會為貴組織的特定環境建立各項基準，進而立即獲得更好的情報，並加速異常活動偵測。將趨勢與基準相比較，可讓您檢視歷史活動模式，以快速建立典型 IT 活動的模型 (亦即正常狀態)，透過這個模型，您可以輕易發現新的潛在性有害趨勢。為了增強這些功能，您可以進一步調整您環境的基準和相應的異常狀況偵測。NetIQ Sentinel 也能顯示您的安全和法規遵循狀況如何隨著時間而改變。
- **彈性的部署選項** – NetIQ Sentinel 以兩種形式提供，第一種是可透過國際標準化組織 (ISO) 影像檔案格式的方式部署於 VMware、HyperV、XEN 等各大監管程式的軟體裝置，另一種是可安裝於 SUSE® Linux Enterprise Server 和 Red Hat Enterprise Server 平台上的軟體。NetIQ Sentinel 的部署與授權模式極具彈性，可讓您在整個企業組織中部署 SIEM 與記錄管理，以符合其特定使用需求。Sentinel 使用彈性的搜尋與事件轉遞機制，使部署架構能配合您的環境，即使是高度分散的部署方式也能支援。
- **高效能儲存架構** – NetIQ Sentinel 採用最適合長期事件歸檔的高效率檔案式事件儲存層。事件儲存區提供 10:1 的壓縮比，並經過索引，充分支援快速搜尋。此外，NetIQ Sentinel 還可讓您選擇將貴組織部分或全部的事件資料同步或移動至傳統的關連式資料庫。透過大幅增強的搜尋功能，您尋找資料和產生報告所花費的時間縮短了。有了 Sentinel 儲存架構，您再也不需要購買第三方資料庫授權，進而降低組織的整體擁有成本。


NetIQ Sentinel 7 利用身分識別管理，將使用者與系統中的特定動作相連結，提供領先業界的使用者活動監控功能。

- **圖形化的規則產生器** – NetIQ Sentinel 能讓您直接使用在您的環境中收集到的事件，快速建立事件關連規則，管理員無須接受大量訓練，或是學習專屬的程序檔語言。另外，您可以在部署規則前先進行測試，以減少誤判的警告、改進事件關連情況，從而獲得更完善的入侵偵測功能。這不僅能讓企業組織更快實現價值，同時還能降低整體擁有成本。
- **強化的身分識別功能** – 透過與 NetIQ® Identity Manager 的內建整合，NetIQ Sentinel 成為業界唯一與身分識別管理緊密整合的產品，能將使用者與企業中的特定活動相連結。在安全資料中附加使用者和管理員唯一的身分識別資訊，能讓您更清楚掌握存取系統的人、時、地。此外，藉由將身分識別資訊納入事件資料，NetIQ Sentinel 不僅能聰明地防範內部威脅，還能提供一套更容易施行的回復機制。NetIQ Sentinel 也和 Microsoft Active Directory 的身分識別整合，未來也將陸續增加與其他身分識別管理產品的整合。
- **簡化的過濾、搜尋與報告** – NetIQ Sentinel 簡化 IT 基礎架構事件的收集，自動執行冗長繁複的法規遵循稽核與報告功能，並大幅縮減尋找和準備稽核員所需資料的複雜性、時間與成本。這有助於企業組織快速達成政府法規與業界規範的要求。
- **經過強化與擴充的套裝報告** – NetIQ Sentinel 透過資料彙總與標準化功能、預先建立的報告、可自定的規則，以及快速搜尋功能來簡化報告作業。只要按下按鈕，即可隨時根據即時搜尋結果產生報告，讓您針對所需要的資料立即產生報告，無須費力修改限制重重、預先建立的樣板。
- **整合式單一解決方案** – NetIQ Sentinel 將記錄管理與 SIEM 結合為單一整合式解決方案。

*「要跟上網路安全活動急遽增加的速度，至少需要 10,000 名人員。Sentinel 讓我們的中央監控團隊能夠完整、全面地檢視安全活動，因此我們便能夠立即針對最緊急的事件採取行動。」*

**Keith Rohwer**
NCDOC 的研發、測試和評估主管

NetIQ

欲進一步瞭解
NetIQ Sentinel 7，
或欲開始試用，請造訪
**www.netiq.com/sentinel7**。

## 主要獨特優勢

簡易型的 SIEM 解決方案固然執行簡單，但無法提供實在的安全情報，而傳統的 SIEM 解決方案儘管功能強大，卻講求高度的技能與繁瑣的自定作業，且難以適應不斷變遷的環境。NetIQ Sentinel 7 與這兩者不同，本產品可以展現安全情報的最高價值，因為它簡單易用，卻蘊含強大功能，有助於回答這個問題：「我的安全有保障嗎？」

- 提供虛擬軟體裝置封裝的部署方式，部署快速又簡易。虛擬裝置與硬體式選項不同，可以輕易擴充以因應成長、增加容量。
- 具備強化的身分識別功能，可提供豐富的安全事件相關背景資訊，讓您在偵測與防範內部威脅時，能夠掌握更深入的情報。
- 提供圖形化的規則建立介面與容量規劃，管理上更加簡單。管理員可在系統導入期間快速建立關連規則，並隨著日後業務需求的變遷，輕鬆維護、更新規則，降低整體擁有成本。
- 產品安裝完成後，安全情報儀表板可隨即投入運作，開始監控企業組織的安全狀況，因此產品導入首日即可實現價值。
- 安全管理員可以透過直覺式的資料搜尋方式，輕鬆找到所需資料，並將搜尋結果快速轉換為報告。

**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：



PB595001SENT ENG A4 PO 5/12 F
577-TW1002-002 DS 06/07