NetIQ

Flyer
Change Guardian

NetIQ Change Guardian

監控特權使用者的活動，降低內部威脅與目標式攻擊的風險。

NetIQ Change Guardian 能在最佳時機向適當的利益相關者提供正確資訊，藉此協助辨識及降低安全威脅，並保護企業資產。

在日常生活中，只要特權使用者在IT基礎架構中對重要的檔案、系統和應用程式做出未經授權的變更，組織都會面臨更高的資訊安全風險。

NetIQ® Change Guardian™ 能即時監控重要的檔案、系統和應用程式，藉以偵測特權使用者所進行之未經授權的活動，並協助組織大幅降低重要資產所面臨的風險。本解決方案也能協助您遵循各項法規與隱私權標準，例如支付卡產業資料安全標準 (PCI DSS)、健康保險及責任法案 (HIPAA)、經濟與臨床健康資訊科技法 (HITECH)、國際標準化組織 (International Organization for Standardization) 的最新標準 (ISO/IEC 27001) 及歐盟隱私權指令等。

產品綜覽

NetIQ Change Guardian 可提供您所需要的安全情報，助您迅速辨識並因應可能違反安全規範或導致違反合規的特權使用者活動。它能針對重要檔案、系統和應用程式中未經授權的存取和變更發出智慧型警示，藉此協助安全團隊即時偵測並因應潛在威脅。NetIQ Change Guardian 能緊密整合現有的安全資訊與事件管理 (SIEM) 解決方案，擴大其偵測和因應威脅的能力範圍。本解決方案提供豐富的詳細資料，能指出涉及事件的人、事、時、地、物，大幅降低特定目標式攻擊的風險。NetIQ Change Guardian 搭配 NetIQ Secure Configuration Manager™ 使用，可提供合規及授權報告功能；搭配 NetIQ Sentinel™ 使用，則可提供安全事件管理、記錄聚總和鑑識分析等功能。在具備安全管理和法規遵循管理功能的整合式自動化解決方案中，NetIQ Change Guardian 扮演著不可或缺的重要角色。

功能

為了應付因為自備裝置 (Bring Your Own Device，BYOD)、行動和雲端等技術不斷發展而日益複雜的威脅與運算環境，企業組織必須採取多層次的整合式方法來捍衛重要的系統和機密資料。NetIQ Change Guardian 產品提供下列重要的保護措施：

- **特權使用者監控**：稽核並監控特權使用者的活動，降低內部攻擊的風險。
- **即時變更監控**：辨識並回報重要檔案、平台和系統的變更，協助防堵漏洞並確保遵循合規。
- **即時智慧型警示**：讓您在第一時間掌握可能釀成資訊安全漏洞的未經授權變更，用最快的速度來因應威脅。
- **達成法規遵循與最佳實務**：證明貴公司有能力監控重要檔案和資料的存取，協助您滿足合規要求。

功能與優點

NetIQ Change Guardian 不只能辨識變更，還能提供您所需的鑑識報告，協助您作出明智的資安決策，確實將遺失企業資料的風險降到最低。

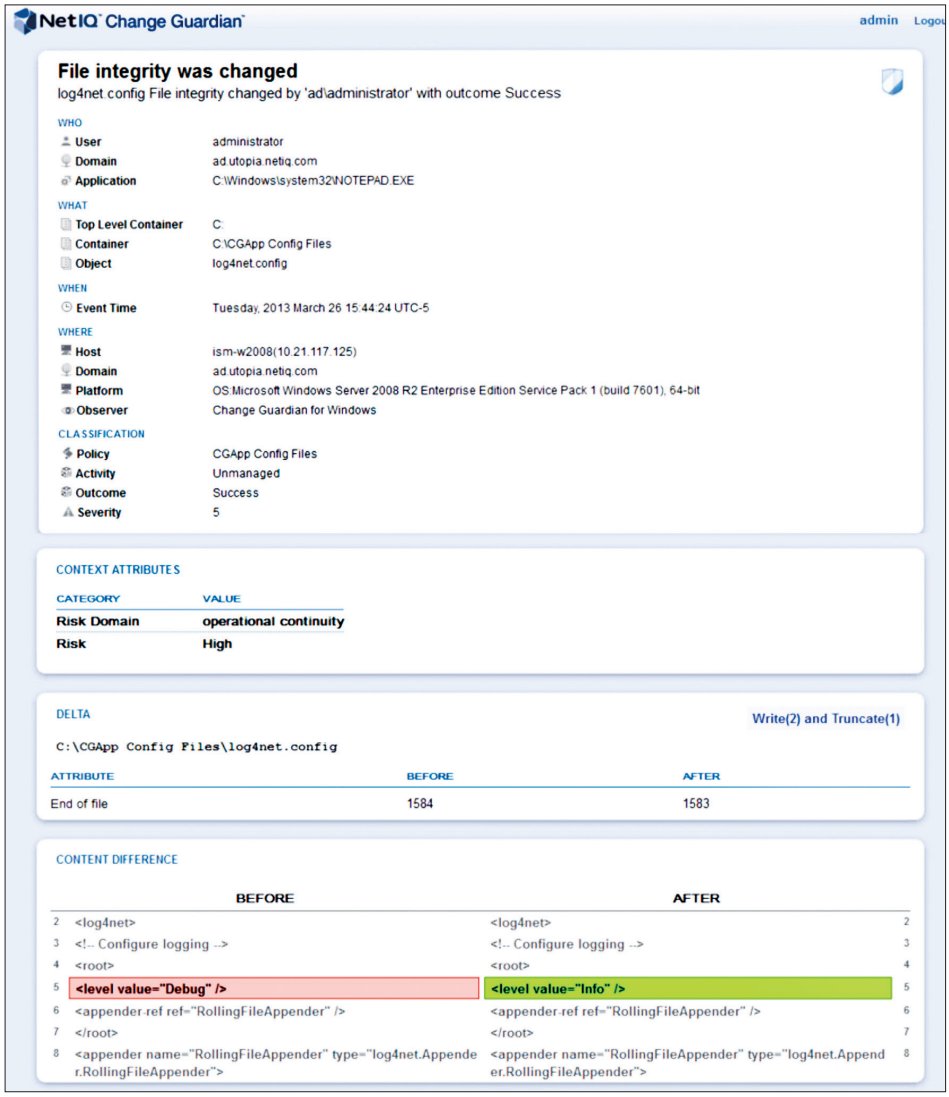
主要功能與優點

- 在 Microsoft Windows 與 Microsoft Azure Active Directory、UNIX 與 Linux 環境中，針對特權使用者活動提供全面且詳細的稽核線索

- 以熟悉的日常用語標明監控原則，讓安全團隊能輕易在 NetIQ Change Guardian 規則與多種規範、要求及內部規則所需之技術控管措施間建立關聯
- 提供豐富的安全事件詳細資料，能指出變更或活動的人、事、時、地和授權狀態，並且包括變更前後的詳細資料
- 辨識受管理與未受管理的變更，並即時對未經授權的變更發出警告
- 辨識主要檔案系統的變更，協助達成檔案完整性監控的合規要求
- 與包括 NetIQ Sentinel 和 Micro Focus ArcSight 在內的各大 SIEM 解決方案緊密整合，讓事件產生關連性並大幅降低未偵測到安全漏洞的風險
- 提供必要的報告工具，明確地向內部和外部稽核人員證明合規成效

主要獨特優勢

- **以全方位的整合式方法**監控特權使用者活動，遏止攻擊行為，讓您的企業得以永續成長。在動態的混合 IT 環境中，通常無法全面檢視風險與合規遵循的情況，因此您需要全方位的資訊安全解決方案，協助您偵測並回應未經授權的變更、活動和存取行為。NetIQ Change Guardian 能免除使用多種工具管理不同系統的需求，進而簡化安全及合規流程。它能集中安全資訊，藉以延伸組織現有的風險管理能力，並防堵及因應營運中斷的狀況。NetIQ Change Guardian 能支援由許多伺服器、作業系統、裝置和應用程式 (包括 Microsoft Windows、Microsoft Azure Active Directory、UNIX 與 Linux) 建構而成的異質環境。
- **擴充 SIEM 的功能**，彌補安全情報的不足。SIEM 解決方案無法提供用來偵測內部威脅與目標式攻擊所



需的安全事件詳細資料，也不提供某些合規要求的檔案完整性變更報告。與 SIEM 解決方案 (例如 NetIQ Sentinel 與 Micro Focus ArcSight) 整合後，NetIQ Change Guardian 可增強 SIEM 解決方案所提供的「可作為行動依據的情報」，使其具備您所需的安全事件詳細資料，讓您迅速辨識並因應威脅。掌握全方位的安全情報後，您更能在釀成重大損害前，率先削弱攻擊所帶來的衝擊，杜絕違法情事。

- **智慧型警示**可協助降低因濫用特權而造成的內部威脅與目標式攻擊風險。NetIQ Change Guardian 能對未經授權就存取和變更重要檔案、系統與應用程式的情況發出智慧型警告，協助您即時偵測和因應潛在威脅。此類警告含有詳細的安全資訊和必要的詳細資料，能辨識威脅並記錄變更。具體資訊內容包括執行動作的人員、內容、時間及地點，也會顯示動作是否獲得授權，並提供變更前後的詳細資料。

- **規則式的監控**能協助您以簡單的方式及更低的成本證明合規要求。NetIQ Change Guardian 藉由規則式的變更稽核和監控，協助您遵循各種法規、要求、最佳實務和內部規則的規範。此解決方案能夠以熟悉的日常用語標明監控原則，讓您得以輕易建立 NetIQ Change Guardian 規則與技術控管措施間的關聯，簡化意義及目的。NetIQ Change Guardian 能以一目了然的簡單方式來呈現活動，減少準備稽核及證明合規所需的作業。

NetIQ Change Guardian 可即時偵測重要檔案、系統與應用程式中未經授權的變更與存取，及早辨識並防堵安全漏洞。

www.netiq.com

NetIQ
台灣網威股份有限公司
台北市大安區 106 敦化
南路 2 段 216 號 26 樓 B 室
Tel. 886-2 23760000

info@netiq.com
www.netiq.com/communities
www.netiq.com

如需本公司在北美、歐洲、
中東、非洲、亞太地區和
拉丁美洲分公司的完整列表，
請瀏覽 www.netiq.com/contacts

www.netiq.com