Identity-Powered Security

將安全保護提升到滴水不漏的程度

智慧型暨整合式身分識別、存取與安全管理

新興技術提高 IT 複雜性

雖然產業持續不斷地在安全防護上加強投資，但是大規模的資料外洩事件卻仍持續占據新聞版面。IT 複雜性的提升 (有部分是因雲端、行動力以及社群身分的普及所導致) 會大幅削弱資安團隊保護機密資料的能力，因為傳統的威脅辨識和漏洞因應方法已不再能有效防範最新一代的網路攻擊。在一些涉及龐大利益的資料外洩案件中，攻擊者通常會取得信任的內部使用者的身分證明，瞭解企業如何管理與監視高權限內部使用者之後，再利用其中的弱點進行攻擊。

必須修補的安全情報漏洞

若要強力防範日漸增長的「內部威脅」，首先必得依最佳實務實施更嚴密也更符合業務需求的存取控制。簡而言之，對於所有使用者均僅給予最低限度的權限，並且將授權使用者人數降到最低。確立這些控管機制後，接著必須監控授權使用者，確保他們的活動均正常且符合業務需求。

安全監控傳統作法的一大問題，即是在 IT 基礎架構擴大，不斷添增各種工具的情況下，同時也會產生更多的安全事件「雜訊」。早已人手不足的資安團隊於是必須分析、理解堆積如山的資料。授權使用者的活動常因此而埋沒在「雜訊」中，而這種狀況容易讓人無法正確掌握什麼是正常使用者行為。資安團隊會開始錯失可能表示有攻擊發生的關鍵性指標。當資安團隊因為安全分析不足 (或欠缺)，而無法掌握可能代表威脅的活動與事件時，即構成所謂的安全情報漏洞。

若要解決此問題，就必須採取整合式安全策略，將使用者與事件的額外背景資訊整合到安全監控解決方案中。藉由分析這些背景資訊，即可抑制事件「雜訊」並偵測到異常的活動。「身分識別」是一大關鍵背景資訊來源，掌握身分識別就能瞭解組織內的正常使用者行為。當使用者的「身分識別」整合於各項安全措施，即可辨識哪些使用者擁有不當存取權限，並加以監控、管理，避免內外攻擊者帶來不必要的風險。

來源：《2014 年北美及歐洲網路威脅防禦報告》(Cyberthreat 2014 Defence Report North America & Europe)。

以 Identity-Powered Security 建構強大防禦機制

Identity-Powered Security 就是將身分識別資訊整合到安全監控與漏洞因應措施當中。這種作法結合身分識別管理、存取管理以及安全事件管理，針對使用者的身分、哪些活動屬於正常行為及使用者需要存取哪些內容，提供完整的組織知識。Identity-Powered Security 能讓團隊突破日常活動的雜訊，迅速辨識使用者的行動屬

NetIQ

於正常而可接受，或是異常而有害的行為。加入這些「身分識別背景資訊」之後，安全資料就會變成可作為實際行動依據的安全情報，讓團隊能用以遏止攻擊，並加快回應事件的速度，避免造成傷害。

NetIQ、身分識別與您

NetIQ 是全球領導級的身分識別、存取及安全管理解決方案供應商。每一天，我們都發揮廣泛的經驗與專業，為客戶提升機密資產與服務的能見度及存取控制能力 (不論資產位於何處、使用者是誰)，進而協助客戶有效而快速地因應最複雜的威脅。

NetIQ 能幫助您實現 Identity-Powered Security，為您提供必要工具以彙總整個 IT 基礎架構的身分識別資訊，並將這項資訊整合至您的安全監控工具，提供必要的「身分識別背景資訊」，讓團隊能夠以超乎先前想像的頂尖速度有效辨識與因應潛在的攻擊。

NetIQ 是為您提供智慧型暨整合式身分識別、存取及安全管理解決方案的最佳夥伴。以下僅是我們協助客戶保護資訊安全、讓組織符合法規的眾多方法中的一小部分。

快速獲得適當存取權限	限制授權使用者可能引發的風險	以更快的速度偵測到漏洞	報告並遵循法規
• 將身分識別、佈建和核准程序自動化，讓您的使用者在工作第一天就獲得適當的存取權限。 • 在員工離職或調動職務時立即撤銷存取權限，以降低資料遺失的風險。 • 確保僅授予及強制執行最低限度的權限，以遵循法規，並在所有系統維持一致的身分識別。 ***NetIQ 解決方案*** • NetIQ® Identity Manager • NetIQ® Access Manager™ • NetIQ® CloudAccess	• 限制 Active Directory、Windows、Linux 或 UNIX 系統的授權存取，並報告管理員所進行的活動。 • 即時監控重大資產的變更，並加入身分識別情報，幫助您作出更明智的安全決策。 • 監控並報告重大伺服器上的管理員活動。 ***NetIQ 解決方案*** • NetIQ® Directory and Resource Administrator™ • NetIQ® Privileged User Manager™ • NetIQ® Sentinel™ • NetIQ® Change Guardian™	• 提供即時的事件分析以加快辨識及遏止威脅的速度，避免造成傷害。 • 建構安全情報以防範日後攻擊。 • 監控授權使用者對於含機密資料的檔案的存取。 ***NetIQ 解決方案*** • NetIQ® Sentinel • NetIQ® Change Guardian • NetIQ® Privileged User Manager	• 監控使用者活動並強制遵循 IT 法規。 • 偵測並自動覆寫存取規則的變更，且同時遵循 IT 法規。 • 證明存取治理與 IT 法規遵循，並自動化存取權限的審查作業。 ***NetIQ 解決方案*** • NetIQ® Change Guardian • NetIQ® Secure Configuration Manager • NetIQ® Access Governance Suite • NetIQ® Identity Manager

歡迎造訪 **www.netiq.com** 以進一步瞭解 NetIQ 完整產品組合的相關資訊，包括系統及應用程式管理、工作負載管理和服務管理等各式解決方案。

561-TW1003-001 08/14 DS