WHITE PAPER

在雲端世界確保安全

全球組織以驚人的速度紛紛採用雲端運算，這使得現今企業及政府機關的運算基礎架構隨之脫胎換骨，非昔日所可比擬。根據 IT 市場研究公司 IDC 的預測，美國的 IT 雲端服務營業額在 2016 年前將成長至 432 億美元；此市場在 2011 年時僅有 185 億美元。雖然雲端運算毋庸置疑能爲組織節省可觀的成本，並提升營運效率，但同時亦帶來新的風險與不確定性。現在幾乎所有組織都有部署公有雲、私有雲或混合雲的基礎架構。這些組織在排除雲端技術固有安全風險的同時，也需要遵循產業及政府所制定的法規。

所幸近年於資訊安全與法規遵循管理方面的技術有長足的進步，因此能夠爲雲端運算使用者降低風險、改善對威脅的回應速度，並大幅減輕法規遵循管理所耗費的心力。NetIQ 正是其中的開路先鋒。這份白皮書提供三個簡單的步驟，說明如何在移轉至雲端的同時，還能保有可見度與掌控力，並且解釋 NetIQ 如何能夠在各方面提供協助。

NetIQ

NetIQ | WHITE PAPER

目錄

雲端運算的效益

雲端運算在 IT 產業掀起革命浪潮，顛覆了 IT 爲使用者提供應用程式與服務的方式。其採用率的成長速度較傳統軟體快五至十一倍 [1]，且 IT 預算中配予雲端技術的比重也日漸增加。

雲端運算能夠帶給組織許多實質效益，而其中最引人注目的自然就是降低營運成本、提升規模彈性以及改善企業靈活度。

雲端的安全難題

雲端運算雖然帶來許多實質效益，但是要將作業移轉至公有雲、私有雲或混合雲的基礎架構亦有其難處，特別是在安全與法規遵循方面。不變的是 IT 仍需要對安全與法規遵循負起責任，並且在妥善管理企業的同時，繼續於正確的時間、在正確的位置、爲正確的使用者提供商業服務。

降低安全風險

當組織將應用程式與服務移轉至雲端基礎架構時，常誤信此舉本身即可降低網路安全風險；他們認爲雲端提供者都已做好先進的網路安全防護措施。這是非常危險的想法，因爲在保護機密資料的機密性、完整性與可用性方面，以及在證明產業與政府法規的遵循度方面，需求不但永遠不會降低，最終也仍舊是您需自行承擔的責任。完全依賴雲端提供者的防護措施可能造成災難性的後果，這一點我們也在 2011 年 Expedia 的雲端運算資料外洩以及 2012 年 Apple 的 iCloud 資料外洩事件中得到印證。

雖然雲端提供者向來都是部署同級最佳的防火牆與入侵防禦系統 (IPS) 來防範已知的網路威脅，但是這些裝置並無法排除如系統組態錯誤以及系統管理權限設定不當 (和管理不良) 所造成的風險。這些安全風險對雲端代管系統造成的威脅並不下於對實體網路所造成的威脅。看不見的系統，絕不能就不關心。

偵測安全漏洞

IPS 裝置、新一代防火牆 (NGFW)，以及其他比對病毒碼的防禦措施，對於偵測已知威脅都非常有效。有些方式甚至還能偵測到針對已知作業系統與應用程式弱點發動攻擊的未知威脅。不過，現今最複雜、最危險的網路威脅均是透過前所未見的惡意軟體，這些惡意軟體是專爲攻擊作業系統與應用程式中的未知、零時差弱點所設計，我們稱此爲「先進持續性威脅」，簡稱 APT。

監看雲端代管系統是否有安全漏洞，比監看實體電腦網路更加困難。大多數雲端提供者不會讓客戶存取其網路安全裝置的管理主控台或記錄，因爲提供者要利用這些項目，來監控會同時對多用戶虛擬化環境中的許多客戶造成影響的入侵事件。也正因爲如此缺乏可見度，所以客戶難以 (甚至完全不可能) 主動偵測並因應其機密資料所面臨的威脅。

有些組職如雲端安全聯盟 (Cloud Security Alliance, CSA) 已著手制定標準，其目的在於支援雲端安全及稽核資料的彙整，讓客戶對其機密資料擁有更高可見度。只是現階段這些標準仍屬規劃初期，業者無法立即採用。在對雲端機密資料擁有更高可見度之前，IT 團隊仍必須將組織內所建立的資料分門別類，並根據其機密性與價值，指定相關的風險等級。有了這些資料，IT 就能更有效判斷哪些類型的資訊適合讓外部代管，以及管制存取權限所需的規則和程序。

IT 可決定由內部自行保管高度機密的資訊，將其存放於應用程式或私有雲上，藉由集中控管、監控存取人員來預防資料外洩或遭竊。

[1] 「The Top Three Cloud Stocks from Gartner's Magic Quadrant」(Gartner 神奇象限的前三大雲端股)，*The Motley Fool*，2013 年 3 月 7 日。

維持法規遵循

組織即使將應用程式與其他 IT 服務移轉至雲端，仍有責任證明確實遵循產業規定 (如 PCI 與 NERC) 和政府法規 (如 HIPAA、FISMA、SOX、GLBA)。但是，要向外部稽核人員證明雲端環境的法規遵循狀態卻可能非常困難，因爲雲端基礎架構中用來保護雲端基礎架構的許多安全系統均是由雲端提供者提供及監管，而非由組織自行管理。

組織必須確保雲端服務 (不論是私有雲，還是基礎架構即服務 (IaaS)) 中的機密資料受到妥善保護及管理，而且其方法必須符合企業資訊管理政策及產業法規。同時，企業也必須監控並驗證服務等級，確保服務提供者能夠持續提供其承諾的服務等級與客戶經驗。

三個簡單步驟獲得可見度與掌控力

組織不應完全依賴外部雲端提供者的安全防護。在導入雲端技術之前，組織必須主動並持續依最佳實務，在公司內部系統執行安全控管措施，以期達成「準雲端」之狀態。

一套準雲端安全計畫將有助於團隊管理雲端所帶來的複雜度及風險。在採用雲端技術之前，首先緊縮企業內的安全控管、系統與規則，如此團隊就能更有效管理其後雲端技術在使用人數、裝置數、應用程式與資訊交換量等方面無可避免的成長。即使在結合傳統與雲端元件 (如 IaaS 提供者的元件) 的混合式環境中，準雲端安全計畫也能有效調整規模。準雲端安全計畫是採資料導向，著重於降低風險，並協助團隊持續維護其安全與法規遵循狀態。準雲端安全計畫應包含下列項目：

- **變更監控**：變更監控解決方案能夠持續監控、識別並通報重要檔案、平台、應用程式與系統的非預期變更。這些非預期且通常未經授權的變更可能是意外，亦可能是惡意，但是無論如何均會危害整個組織的安全與法規遵循狀態。例如，「檔案完整性監控」(FIM) 即是一種變更監控技術，將關鍵檔案的現狀與已知的良好基線做比對，藉以監看其完整性。FIM 能夠警示 IT 在作業系統或應用程式中可能含有的惡意程式碼，進而偵測可能避開傳統安全防禦措施的先進威脅。

- **安全組態管理**：安全組態管理解決方案可對照法規規定、安全最佳實務以及企業 IT 規則，評估重大 IT 系統的安全組態設定 (如密碼規則遵循、啓用的服務、修補的弱點以及開放的連接埠)，以證明法規遵循狀態並管理資訊安全風險。若其中有任何一個解決方案偵測到有安全設定不符合安全組態管理規則，該解決方案便會警示 IT 以利評估並視需要修正設定。現今的組態管理解決方案讓組織輕鬆「強化」其重要 IT 系統，並在遵循法規之際，繼續保持高強度的安全狀態。

- **授權帳戶管理**：透過精細的權限委派以及管理活動監控，獲授權的帳戶管理解決方案能讓 IT 控管並稽核授權使用者身分證明 (通常爲 Active Directory) 的使用狀況。這些方案可保護組織，防範在未經授權的情況下提高權限，並協助辨識授權帳戶的不當使用行爲。

- **安全資訊與事件管理 (SIEM)**：SIEM 解決方案讓您對組織 IT 安全系統及其相關安全事件的整體狀況一目瞭然。SIEM 平台可從防火牆、防毒 (AV) 平台、IPS 裝置、應用程式軟體與其他各種來源彙整記錄與其他安全相關資料，再將這些異質的資料建立關連，發掘隱藏其中的威脅。

以上四種安全與風險管理解決方案相輔相成，可協助組織改善基礎架構安全並降低風險。除非組織能夠善用這些技術，先保護好內部系統的安全，並協調規劃使其達到準雲端狀態，否則服務移轉雲端時將會面臨更大的風險。

以下三步驟流程整合了變更控管、安全組態管理、授權帳戶管理以及 SIEM 技術，針對內部系統的強化提供實用的工作架構。

第 1 步：降低風險

爲了在雲端系統獲得可見度與掌控力，首先需要降低風險。其作法是縮小基礎架構的攻擊面積、監控系統組態的完整性，並將授權使用者存取權限予以最佳化。

縮小攻擊面積。簡單來說，基礎架構的攻擊面積即是攻擊者能夠未經授權存取系統、執行未經授權的變更並取得機密資料的所有手段之總合。要縮小攻擊面積，IT 必須強化系統安全，妥善設定使用者權限，僅允許使用者存取其業務所必要的應用程式、服務、連接埠以及通訊協定。完成之後，IT 亦需持續監控並評估這些系統，確保其組態不偏離最佳實務。

市面上有許多企業 IT 安全軟體能夠管理並監控直接連上您網路的系統，並執行組態最佳實務。在規劃移轉至雲端之時，您必須詳加審視每一套此類軟體，判斷其在雲端是否仍然有效。這是因爲雲端提供者有可能不支援您在私有環境中所擁有的低階直接存取功能。

善用 IT 安全架構。爲協助組織實現 IT 安全最佳實務，最終達到降低網路安全風險的目標，有一些組織設計了 IT 安全架構 (其中有許多架構獲得產業與政府機構 IT 安全法規參照，這些法規包括 PCI 和 FISMA)。這些架構納入了強化防火牆、路由器、交換器、伺服器、桌上型電腦、筆記型電腦與行動裝置之安全組態的適用準則。一些較常見的 IT 安全架構有：

- SANS 20 個關鍵安全控制項目
- NIST SP 800-53
- ISO 27001
- COBIT

一些知名的安全組態管理解決方案均提供上述四種架構的規則樣板。使用者能夠利用儀表板和報表找出不符規定的主機，並查閱指示以將其修正成爲符合規定之狀態。

最佳化授權存取。大多數專家均同意，當組織賦予 IT 人員管理權限時應遵循「最低權限原則」。最低權限即代表使用者僅應獲得其工作所必要最低限度的使用者權限。可惜的是，並非所有平台都支援精細權限劃分，因此無法真正落實最低權限原則；更有許多平台在設計上使得權限的設定與管理難以執行。此外，單純依賴最低權限並無法降低工作過重或懷有惡意的 IT 人員所帶來的風險。藉由在組織內部及雲端平台與服務上採用頂尖授權帳戶管理技術，IT 組織即可依據精確細分的角色賦予 IT 人員權限，讓每一個角色擁有一項或多項授權 (權限)。此外，爲預防未授權的使用者權限提高，比較好的授權帳戶管理解決方案會採用雙金鑰安全設計，需要經過兩位 IT 管理員的確認，才能將授權帳戶的權限提高。

第 2 步：改善威脅回應速度

強化組織內部與第三方提供者 (如 IaaS 提供者) 的安全組態，並將授權使用者帳戶最佳化之後，繼續維持雲端安全與法規遵循狀態的第二步，即是改善您的威脅回應速度。其作法是偵測來自混合式基礎架構內部的威脅，將這些威脅與其他安全防禦措施所產生的情報建立關連，並監控授權使用者可能發生的存取違規。

偵測內在威脅。在偵測以雲端式主機爲目標的網路威脅時，第一道防線即是雲端提供者的防火牆與 IPS。但是現今會造成最大損害的威脅均是攻擊零時差弱點；您不能再單獨依賴雲端廠商的傳統周邊防禦。

安全團隊不能再偏重周邊防護，因爲傳統的邊界已不再具有意義；反之，他們必須針對資料本身設計安全控管措施，不論資料是儲存於何處。對於保護重要資料、達成法規遵循目標而言，資料導向的威脅防禦措施是最有效的方式，其中最典型的範例就是加密與記號化。安全團隊應將資料導向的概念延伸，涵蓋所有需要頻繁存取重要資料或與重要資料互動的機密系統與使用者。著重於機密系統與使用者的資料導向安全解決方案範例包括監控授權使用者活動是否有異常行爲、是否未經授權存取機密檔案，或是即時監控安全事件與異動，以偵測意外或惡意變更機密檔案及系統的事件。

採用資料導向方法後，安全團隊便能更有效、更主動地偵測潛在威脅，進而降低機密資料與系統所承受的風險。此方法即使當 IT 環境因爲導入破壞性技術 (例如雲端) 而日漸複雜之時，仍然讓團隊能夠可靠獲得安全保障，達成法規遵循與商業目標。

整合安全防禦措施。企業對於 SIEM 技術的採用率在過去十年間呈爆炸性的成長。SIEM 解決方案與基本的記錄監控解決方案不同；基本監控僅將記錄資料彙整，而 SIEM 解決方案則會整合、歸納內部與雲端所有安全防禦措施的情報，爲 IT 提供單一控制台，不但可以此回應日常發生的安全事件，更可用於發現其他難以偵測到的進階攻擊。業界頂尖的 SIEM 平台也與變更監控解決方案緊密整合，提供更豐富的安全情報並加快回應速度。

監控授權存取違規事件。頂尖的授權使用者管理方案不僅能讓 IT 將授權使用者依角色分類，還能將授權使用者活動記錄於安全、唯讀的歸檔中。如此一來，所有授權使用者行動均將留下詳細的稽核線索，包括當有人嘗試未經授權存取系統時 (不論系統是在現地或第三方提供者 (如 IaaS 提供者) 的雲端上)，這可能表示發生 APT 或其他目標式攻擊，授權帳戶遭到入侵。

第 3 步：減輕法規遵循心力

爲了在雲端基礎架構獲得可見度與掌控力，第三個步驟，也是最後一個步驟，即是減輕產業及政府法規遵循所需的心力，這類法規包括 PCI、HIPAA、FISMA、SOX、NERC 與其他各項標準。其作法是遵守相關的 IT 安全架構，善用您的安全組態管理解決方案所提供的原則庫，將法規遵循報表與警示自動化。

遵守 IT 安全架構。如第 1 步所述，許多產業與政府規定的 IT 安全法規均參照常見 IT 安全架構中的最佳實務。藉由同時於實體網路及雲端上善用最佳 FIM 與安全組態管理解決方案，組織即能夠遵守相關的 IT 安全架構，進而減輕達成及維持法規遵循狀態所花費的心力。以下即舉例一些 IT 安全法規及其所參照的 IT 安全架構：

- PCI 參照 SANS 20 個關鍵安全控制項目
- FISMA 參照 NIST SP 800-53
- SOX 參照 COBIT

善用安全組態管理規則樣板。一套安全組態管理規則是由個別的「測試」(以及多組的測試) 所構成，這些測試是描述特定主機組態設定應有的狀態。比較好的產品方案都會隨附規則庫，也就是預先設定的測試集合，其對應至產業及政府各重大法規，包括本文件上文所提及之項目。

將安全組態管理的法規規則樣板對照至需遵循 IT 安全規定的內部主機與雲端式主機 (例如負責處理信用卡交易的主機)，IT 就能夠大幅減輕達成及維持法規遵循狀態所需的心力。

自動化法規遵循報告。大多數頂尖的資訊安全產品，特別是在法規遵循方面扮演特定角色的產品，均提供既定報表以協助證明企業對於產業與政府法規的遵循狀況。比較好的安全解決方案可將法規遵循報告功能予以自動化，自動將法規遵循報表傳送到內部稽核人員與 IT 管理人員手中。

NetIQ 能提供哪些協助

現今網路威脅型態瞬息萬變，而企業與政府機關所面臨的產業及政府法規亦面臨同樣情況。若無合適的工具，要在雲端達成並維持法規遵循狀態將是一大難題 (其實在實體網路上亦將同樣困難)。幸好，NetIQ 能助您一臂之力。

我們知道，過去對於降低資料安全與法規遵循風險的傳統作法已不再有效，我們也知道您需要的是一套全面性的解決方案。本公司的身分識別、存取及安全管理解決方案套件能夠順暢整合，幫助您控管雲端服務與資料的存取，減少混合式環境中的資料外洩風險，同時在雲端環境中確實遵守產業規定與安全規則。

在此就讓我們簡單介紹 NetIQ 五大產品，看看它們如何有助於執行前述的三個步驟，協助您達成並維持企業安全與法規遵循狀態，讓您做好萬全準備迎接雲端時代的到來。

NetIQ® Change Guardian™

NetIQ Change Guardian 提供授權使用者活動與變更監控功能，協助 IT 專業人士即時偵測並回應潛在的威脅。此解決方案可監控整個分散式環境，並警示告知任何異動，讓您掌握 Active Directory、檔案、目錄、檔案共用、(Windows 主機上的) 登錄機碼、系統程序及其他各種資源的細節分析。警示訊息中亦註明該動作是否經授權，並記載變更前後的詳細資料。NetIQ Change Guardian 以充足的細節提供豐富的安全資訊，其資訊足以辨識威脅並記錄異動，比起單獨使用原生記錄事件，能提供更高的精確度和清晰度。

NetIQ Change Guardian 透過以下功能，協助組織保護其混合式基礎架構並維持法規遵循：

- **授權使用者監控**。記錄授權使用者 (例如網路架構師、管理員) 的活動，降低內賊攻擊的風險。
- **即時變更監控**。即時監控重要檔案、平台、應用程式與系統的變更，預防資料外洩並確保規則遵循度 (包含檔案完整性監控)。
- **未經授權變更警示**。當偵測到未授權變更，可能涉及 APT 或其他目標式攻擊時，即提供智慧警示。警示中提供充足的細節，可識別威脅並記錄變更；詳載例如*誰*執行該動作、執行了*什麼*動作、*何時*執行動作，以及*在哪裡*執行動作。
- **法規遵循報告**。自動提交報表，證明您有能力監控重要檔案與資料的存取，滿足產業及政府法規遵循規定。

NetIQ Secure Configuration Manager™

NetIQ Secure Configuration Manager 能夠定期評估並報告系統組態的變更，並將組態與法令規定及最佳實務原則進行比對，協助確保公司遵循 SOX、PCI、HIPAA、FISMA、NERC 以及其他各種規定。其使用者授權報告功能可評估使用者權限，讓您知道誰擁有存取權，以及他們對重要資訊的存取權限等級，幫助您降低內賊威脅。

NetIQ Secure Configuration Manager 透過以下功能，在保護混合式基礎架構及證明確實遵循 IT 安全法令方面扮演重要角色：

- **組態評估**。提供可自定的規則樣板，能夠配合數十種 IT 架構及法規標準使用，並持續將目前系統組態比對已知的良好基準。幫助您縮小網路攻擊面積並證明法規遵循狀態。
- **使用者授權報告**。評估使用者對於重要系統的存取權限，協助稽核人員瞭解誰能夠存取什麼等級的重要資訊。
- **企業例外管理**。當特定系統必須合理偏離既存認可的組態標準時，此功能可隱藏這類的組態警示，並記錄這類例外狀況的理由。
- **安全及法規遵循儀表板**。透過可自定的儀表板，迅速並且直覺化傳達目前系統的安全與法規遵循狀態，同時滿足多位利益相關者的需求。

NetIQ Privileged User Manager

NetIQ Privileged User Manager 可在所有 Windows、UNIX 及 Linux 環境中，提供授權使用者管理及追蹤功能，進而限制未授權的交易和對機密資料的未授權存取。它讓管理員可集中定義授權使用者能於平台上執行的指令，確保只有授權使用者能夠執行特定的管理工作。

NetIQ Privileged User Manager 透過以下關鍵功能，保護機密資產並證明產業法令的遵循狀態：

- **簡化規則管理。**讓您使用 Web 式主控台集中建立安全規則，再將這些規則施行於所有受管理的 UNIX、Linux 及 Windows 系統上。
- **主動風險管理。**記錄並重現使用者活動，甚至下探至按鍵動作層級，並提供功能強大的風險分析工具。
- **持續性的法規遵循。**提供永久性的稽核記錄以及自動化的資料篩選，協助證明法規遵循狀態。自動將異動加入永久稽核記錄，並篩選資料以確保高風險事件立即醒目可見。

NetIQ Directory and Resource Administrator™

NetIQ Directory and Resource Administrator 是一套功能完備的授權帳戶管理解決方案，負責媒介 Microsoft Active Directory 的存取，限制使用者在整體目錄的特定檢視中僅可執行特定動作。它也支援使用者佈建及其他自動化作業，同時協助執行安全規則及職責劃分。

NetIQ Directory and Resource Administrator 透過以下功能，協助保護資產安全並證明法規遵循：

- **精細存取控管**。透過逾 60 種角色及 300 種權限，協助您精密地指定 Active Directory 權限給 IT 使用者。
- **授權提高控管**。透過雙金鑰安全設計，需要兩位 Active Directory 管理員確認使用者權限異動，預防未授權的授權提高行爲。
- **受控自助服務作業**。讓終端使用者自行更新個人目錄資訊並重設個人密碼，以降低成本。
- **集中式活動記錄與報表**。透過集中記錄所有管理動作，並提供富有彈性的全面性報表，證明法規遵循狀態。

NetIQ Sentinel™

NetIQ Sentinel 是一套功能完備的 SIEM 解決方案，能夠簡化 SIEM 技術的部署、管理和日常使用。NetIQ Sentinel 能夠隨時適應動態的企業環境，不論是在內部或雲端，都提供安全專業人員所需並可作爲行動依據的真正情報，讓他們迅速瞭解威脅情勢並制定回應優先次序。

NetIQ Sentinel 讓安全分析師能夠監控系統完整性，同時爲稽核人員提供全面性的報告功能，持續證明法規遵循狀態。關鍵功能包括：

- **安全情報彙整**。從整個 IT 環境 (包括防火牆、AV、IPS 裝置、安全電子郵件與 Web 閘道、資料遺失預防 (DLP) 系統、應用程式、資料庫等等) 全面彙整記錄資料與其他安全及網路情報。
- **異常狀況偵測**。透過廠商提供及客戶自建之強大關連規則，自動辨識組織實體、虛擬及雲端環境中的不一致。讓您將「正常」網路流量設爲基準，以偵測可能存在威脅的異常狀況。
- **身分識別強化**。透過與 NetIQ Identity Manager 整合，在整個企業中，將特定活動及安全事件與使用者連結。
- **簡化法規遵循報告**。將繁瑣的法規遵循報表功能自動化，同時滿足內部及外部法規遵循稽核人員的需求。

總結

雲端運算正改變企業與政府機構爲他們所服務之使用者提供 IT 服務的方式。但是，雲端運算雖能降低成本、提升規模彈性並改善企業靈活度，但同時也讓保護重要系統以及證明產業和政府法規遵循狀態更加困難。擴大應用雲端與其他商務技術，可能會讓您早已繁雜無比的 IT 環境更加複雜，進一步增加您對於第三方提供者的相互依賴性及整合作業。

組織若能在自身現場環境中先實行前述的三步驟程序，就能夠安全發揮雲端運算基礎架構的效益。一旦達成此目標，您便能夠根據需求，將合適的控管機制與程序直接延伸至雲端。組織依循此程序，便能夠獲得所需的可見度與掌控力，在現場與第三方提供者系統所構成的混合式環境中，有效保護機密資料的安全。此外，組織也能夠維持長久以來努力達成的法規遵循狀態。

NetIQ 榮獲獎項肯定的安全與法規遵循解決方案相輔相成，並能夠配合您既有的 IT 安全基礎架構，協助您的組織達成並維持安全與法規遵循狀態，即使在雲端環境亦然。

關於 NetIQ

NetIQ 是全球性的企業軟體公司，提供身分識別與存取管理、安全及資料中心管理等解決方案，滿足混合式 IT 的需求。利用本公司解決方案，客戶與合作夥伴可在今日複雜且瞬息萬變的 IT 環境中掌握商機。透過適當協調技術與服務供應方式，本公司客戶更能跟上市場腳步，創造更遠大的策略價值。

若要進一步瞭解本公司獲獎肯定的軟體解決方案，請瀏覽 www.netiq.com。

562-TW1014-001

全球總部
1233 West Loop South, Suite 810
Houston, Texas 77027 USA
全球：+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**分公司的完整列表**，請瀏覽 **www.netiq.com/contacts**。