白皮書

降低資料外洩風險：可確保 PCI DSS 法規遵循與資料安全的檔案完整性監控系統

迅速偵測及協助修正資料外洩的能力，是任何資安計畫的關鍵所在。然而每天都有機密企業資料在無偵測機制的情況下外洩。無論資料外洩是網路駭客利用目標式攻擊犯案的結果，或是授權使用者所犯下的無心之過，後果都相當嚴重。如果安全漏洞長期存在而無人知曉，造成的影響還可能會繼續擴大。

本文討論檔案完整性監控 (FIM) 的重要性，其可協助偵測網路駭客的攻擊和內部威脅，以防堵可能損失慘重的資料外洩事件。本文另亦探討檔案完整性監控在遵循支付卡產業資料安全標準 (PCI DSS) 方面所扮演的關鍵角色，並說明 NetIQ 如何透過 NetIQ 身分識別與安全管理系列產品，因應資訊安全與法規遵循的挑戰。

NetIQ

白皮書

目錄

簡介

俗話說得好：「小心駛得萬年船」，現在正是這樣的一個年代。儘管企業的警覺心越來越高，並且也實施了許多資安保護措施，但資料外洩事件仍常登上新聞頭條。事實數據非常驚人：根據 Verizon Business RISK Team 的 Data Breach Investigations Report (資料外洩調查報告，DBIR)，在過去九年間總共發生了超過 2,500 起資料外洩事件，共 11 億筆記錄遭受入侵[1]。更令人憂心的是，這些外洩事件都是在有資安團隊的情況下發生的。以 Heartland Payment Systems 的案例為證，約有 1 億個信用卡帳戶的資訊，在無人知曉的情況下，外洩時間竟然長達 18 個月之久[2]。

檔案完整性監控：安全難題中的關鍵環節

機密企業資料所受到的威脅具有不斷演變的性質。有鑑於此，檔案完整性監控 (FIM) 已成為安全難題中的關鍵環節。時至今日，新式攻擊者已然崛起，其為有組織的犯罪集團，採用系統化與按部就班的手段入侵系統，並在神不知鬼不覺的情形下長期潛伏，藉此達成特定目標。除了立即獲利之外，這些集團還往往另有所圖。以上情境被稱為持續不斷的進階威脅 (APT)。其慣常採用的伎倆，多是利用信任關係漏洞，像是透過合法帳戶來存取及攻擊目標系統。若要保護機密企業資料不受這類威脅的危害，就需要建構包括 FIM 在內的多層防護網。

根據 2013 DBIR (2013 年度資料外洩調查報告)，14% 的資料外洩與內部人員有關[3]。在絕大多數的案例中，都有證據明確指出，權限濫用是發生大規模資料外洩事件的前兆。表面上威脅看似來自內部，但實際上卻可能是因為外來攻擊者侵入系統 (例如利用惡意軟體感染系統) 並假扮成系統內部人員，要想加以區分簡直難上加難；因此這類內部威脅影響所及層面自然是更加廣泛。

根據 Verizon 的報告，這些案例多半有固定模式可循。攻擊者首先會侵入受害者的網路 (可能是透過竊取而來或防護不周的身分證明)，並且在系統上安裝惡意軟體以收集資料。儘管使用自製惡意軟體進行攻擊的手法現在已有固定模式可循，但惡意軟體本身也變得越來越難偵測，因此還是能成功躲過標準惡意軟體防護程式的控管。這也正是自製惡意軟體能在 Heartland 外洩案例和其他重大信用卡資料外洩案例中得逞的原因。

Forrester Research[4] 指出，減少此類攻擊風險的最佳方式，就是部署檔案完整性監控工具，以在系統遭植入未授權軟體或關鍵檔案被授權使用者修改或存取時，立即發出警告。

部署 FIM 軟體不僅是有助於防護安全漏洞的最佳實務作法，更是支付卡產業資料安全標準 (PCI DSS) 的要求。PCI DSS 標準特別要求部署 FIM 軟體，以便相關人士能獲得警告，知悉

1 Verizon Business RISK Team，《2013 DBIR》(2013 年度資料外洩調查報告)，2013 年 4 月，http://www.verizonenterprise.com/DBIR/2013/。
2 John Kindervag，《PCI X-Ray：File Integrity Monitoring》(支付卡產業的 X 光：檔案完整性監控)，Forrester Research，Inc.，2009 年 10 月 26 日，http://www.forrester.com/rb/research。
3 Verizon Business RISK Team，《2013 DBIR》(2013 年度資料外洩調查報告)。
4 John Kindervag，《PCI X-Ray：File Integrity Monitoring》(支付卡產業的 X 光：檔案完整性監控)。

關鍵系統檔案、組態檔案或資料遭到未經授權的修改。FIM 可偵測系統檔案是否遭受未經授權的存取及變更，因此能減少以下風險：

- **資料外洩** – 尤其是因濫用特許存取權限。
- **系統無法使用** – 因檔案、系統與應用程式遭受意外或未經授權的變更。
- **未遵循法規** – 因未能善盡職責監督機密資料的存取及變更。

FIM 是任何資安計畫成敗的重要關鍵。

細說內部威脅

從最基本的層面來劃分，內部威脅有兩類：惡意與非惡意。

非惡意的威脅包括因犯錯、判斷有誤或非故意性舉措而導致關鍵系統或資料暴露在外。上述情況有可能是在使用電子郵件或其他應用程式時發生，也可能是因為筆記型電腦與智慧型手機遺失或遭竊而造成。由於員工和公司擁有的行動裝置紛紛納入資安範疇中，現有的安全控管措施與防禦策略可能已無法勝任防堵資料由這些媒介外洩的工作。因此，非惡意性質的內部威脅逐漸成為人們關注的議題。

至於懷有惡意的內部人員通常是受到金錢利益的誘惑或是對雇主的不滿而產生動機，長期下來，他們可能造成重大損害，並且造成外部的安全漏洞。歷史證據顯示，殺傷力最大的安全漏洞往往來自於擁有較高權限但卻未受到有效監控的授權使用者，或是那些存取權限終其身分識別生命週期都未獲得妥善管理的使用者。Verison Business 指出，心存不滿的員工濫用仍然有效的操作權限，是每年屢見不鮮的資安漏洞案例。

牟利性質的網路攻擊

過去十年來，有幾起造成重大財務損失的安全漏洞是肇因於由老練駭客策畫、具有針對性且量身訂作的攻擊。Heartland Payment Systems 的資料外洩事件就是這類攻擊的最佳例證。本案的資料外洩規模之大，根據資安專家估計，可能有 650 家金融服務公司所發行的 1 億張信用卡受害。Heartland 因此受到毀滅性的財務衝擊，市場資本額蒸發 3 億美元，直接損失更是超過 3 千萬美元[5]。

Stuxnet 蠕蟲是另外一項多媒介精密攻擊的好例子。Bruce Schneier[6] 指出：Stuxnet 蠕蟲「是一種劃時代的惡意軟體，它以極為隱密的方式利用未修補的弱點，並且採取縝密的多管齊下攻擊策略，因此破解該蠕蟲的資安研究人員認為，這有可能是出自有國家政府為其撐腰的專業人士之手。」截至目前為止，該計畫似乎摧毀了伊朗大約五分之一的核子離心機，這雖然未能摧毀該國發展核武的能力，但仍舊發揮了延緩的效果[7]。由於這種蠕蟲原本是用來滲透工業控制系統，因此專家警告，它可能會被當成設計藍圖，進而發展出破壞發電廠、電力網路和其他基礎建設關鍵機器設備的變種蠕蟲。

5 John Kindervag，《PCI X-Ray：File Integrity Monitoring》(支付卡產業的 X 光：檔案完整性監控)。
6 Bruce Schneier，《Schneier on Security：The Stuxnet Worm》(Schneier 的資安講座：Stuxnet 蠕蟲)，http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html (2011 年 2 月 10 日資料)。
7 William J. Broad、John Markoff 與 David E. Sanger，〈Israeli Test on Worm Called Crucial in Iran Nuclear Delay〉(以色列蠕蟲試驗竟成延緩伊朗核武發展關鍵)，《紐約時報》，2011 年 1 月 15 日，http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (2011 年 2 月 10 日資料)。

獵捕網路駭客

駭客攻擊技巧的最大轉變之一，就是在精密攻擊中展現出的高度隱匿能力。這使得安全漏洞會在無人知曉的狀態下存在很長一段時間，而目標系統則將在此期間平白遭受荼毒。以 Heartland Payment System 一案為例，安全漏洞存在了 18 個月才被發現。在當時，Heartland 的內部資安團隊仍舊一無所悉，還是靠著第三方的發現才使整起事件曝光。

這類的精密攻擊會以各種不同的面貌出現，並且採用多重攻擊媒介。然而，一般的線上詐騙攻擊還是有幾個共同的步驟與特性可以辨認。大多數案例都至少存在著前哨偵查的若干跡象，其中大多是以系統線索收集、掃描與列舉的形式出現。受害組織的邊防一旦淪陷，超過 60% 的駭客都能在短短數分鐘或數小時內侵入系統。

而根據 Verizon 報告，在大約 66% 的案例中，機關組織需要數月甚至更長的時間才會發現安全漏洞。就算偵測到安全漏洞，通常也是透過信用卡公司的後端監控所發現，而信用卡公司通常是利用一種稱為疑似偽卡側錄點 (CPP) 的方法來檢測詐騙。

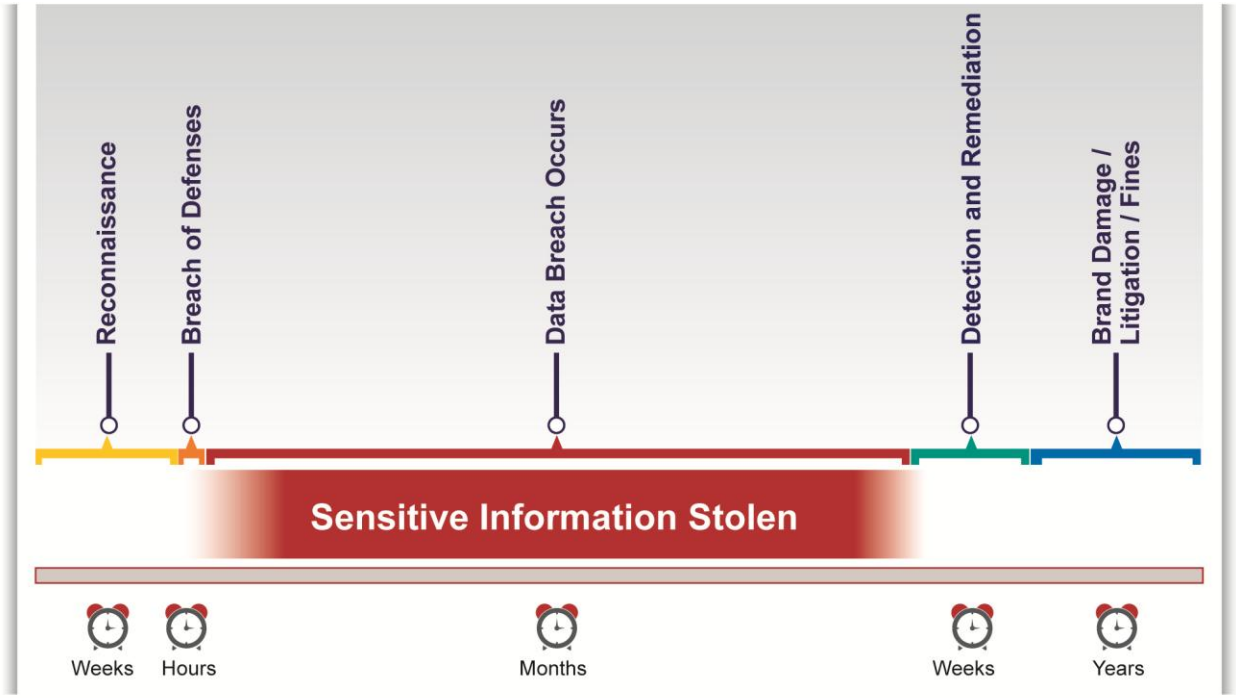

圖 1：典型的資料外洩時程表

對抗威脅：由內部杜絕外來入侵

內部人士涉及的資料外洩事件比起去年有所增長，總是令人不禁懷疑內部攻擊是否正逐漸風行。無論成長的原因為何，其實只要採用幾項簡單的策略，就能確實保護企業機密資料。從 Verizon 報告中，我們知道員工常被賦予超過履行職責所需的權限，而授權使用者的活動也經常未獲得妥善監控。解決上述問題的方法很簡單，就是即時監控授權使用者，以識別未經授權或不尋常的活動。由於授權使用者常會獲得機密或關鍵系統與資料檔案的存取權限，採用 FIM 技術將有助於追蹤關鍵系統檔案、安全記錄檔案、機密資料檔案或共用內容的存取與變更。而在處理關鍵業務系統的系統檔案，或機密資料檔案時，可以設定即時的變更警告，以便在第一時間發現問題。

請注意，一旦攻擊者成功盜用了內部使用者的帳戶，其行為便難以與其他合法活動區別。FIM 的使用或許可偵測出 APT 相關檔案的修改。接下來，您便可搶先在安全漏洞造成更多損失前，立即介入調查此活動。資安團隊如能及早偵測到這類威脅，便可早早做出回應，並且抑制任何隨之發生的損害。

企業法規遵循案例：PCI DSS

除了協助減少資料外洩的風險之外，法規遵循是進行檔案完整性監控的另一項理由。支付卡產業資料安全標準是處理 Visa、MasterCard、Discover、American Express 與 Diner’s Club 等持卡人資訊的公司在契約上的要求[8]。PCI DSS 在第 10 與第 11 條規範中指明使用 FIM。

第 10.5 條確保稽核線索 (記錄檔案) 的安全

> *「針對記錄檔使用檔案完整性監控或變更偵測軟體，以確保現有記錄資料遭到變更時一定會觸發警告 (但新增資料時不應產生警告)。」*

根據 PCI DSS 規範第 10.5 條的規定，企業組織必須針對記錄檔使用檔案完整性監控或變更偵測軟體，且任何變更均必須觸發警告。這項規定有助於保障稽核線索的安全。

第 11.5 條存取及變更重要內容與系統檔案

> *「部署檔案完整性監控軟體，針對關鍵系統檔案、組態檔案或內容檔案在未授權情形下遭到修改的情事，警告相關人員；以及將軟體設定為至少每週執行一次重要檔案比對作業。」*

PCI DSS 規範第 11.5 條旨在為企業提供堅實的安全防護，避免關鍵資源 (尤其是伺服器) 遭到有心人士入侵。企業若要確實保障關鍵系統的安全，必須能掌握檔案與檔案系統的變更，並有能力記錄下列資訊：

- 變更者身分
- 變更的項目：檔案、登錄或組態設定
- 變更時間
- 變更前的值
- 變更後的值
- 此變更是否經過變更管理程序的授權

8 PCI Security Standards Council，LLC，《About the PCI Data Security Standard (PCI DSS)》(關於 PCI 資料安全標準 (PCIDSS))，https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (2010 年 3 月 29 日資料)。

為確保資訊安全與法規遵循的 FIM 管理：NetIQ Change Guardian

資安專家如今所面臨的威脅相當複雜。無論是癱瘓式的惡意軟體攻擊，或是內部人士未經授權存取機密資料，透過 FIM 解決方案即時偵測機密檔案與系統的存取與變更，均可大幅減輕關鍵資料與基礎架構所面臨的風險。

企業導入 FIM 後，除了能在保護機密資料方面做出重大進展之外，亦可確保遵循要求使用檔案完整性監控解決方案的法規，進而避免未遵循法規時的高額罰款和其他負面效應。

NetIQ® Change Guardian™ 採用的即時檔案完整性監控方法具有以下特性：

- 即時偵測關鍵系統與檔案的變更。
- 即使內容僅被檢視而未遭到變更，仍可發出警告。
- 將警告功能整合至 NetIQ Sentinel™ 等頂尖安全資訊與事件管理 (SIEM) 解決方案。
- 確保警告程序提供豐富的資訊，例如變更時間、變更者身分、變更內容，以及變更前的狀態。
- 證明企業監控機密資料存取情形的能力，以協助達成法規要求。
- 偵測大多數平台上的變更：Microsoft Windows、Active Directory (包括群組規則物件)、UNIX 與 Linux。

NetIQ Change Guardian 可即時偵測在重要檔案、系統組態與 Active Directory (包括群組規則物件) 上所發生的未經授權存取及變更行為，以確保您的資安團隊能主動保護企業機密資訊與客戶資料，不受惡意攻擊與意外損害影響。上述解決方案能提供當機立斷所必要的資訊，限縮企業資料外洩風險，並使現存安全投資的報酬率最大化。

雙管齊下：NetIQ 身分識別與安全管理解決方案

關鍵系統與基礎架構中如果有組態變更未受管理，將會使企業組織資料、客戶資訊與系統穩定性承受重大且持續升高的風險。而 NetIQ Change Guardian 正好可以強化您偵測任何未受管理變更的能力，並且有效率地加以回應，大幅降低惡意活動的風險，支援您進行全方位的資料防護。

NetIQ 提供的整合式解決方案可以讓資安團隊建置更完善的資訊安全與法規遵循基礎架構，使其具備可調整性並減輕工作負載。NetIQ Change Guardian 可搭配最頂級的工作流程自動化工具，以及精密控制管理存取權限的 NetIQ® Directory and Resource Administrator ™，形成功能強大、整合完善的自動化身分識別與安全管理解決方案。NetIQ Change Guardian 亦可緊密整合 SIEM 解決方案，例如獲獎肯定的 NetIQ Sentinel，以即時呈現豐富而適切的關聯式資訊給資訊安全與法規遵循團隊。合併使用上述產品不僅能協助公司企業保護資料，也符合 PCI DSS 等重要法規的規定。

結論

FIM 能夠快速偵測關鍵系統遭未經授權存取的狀況，因此是防止自製惡意軟體攻擊與惡意 (或非惡意) 內部活動造成資料外洩的關鍵所在。FIM 也是 PCI DSS 法規遵循的重要一環，在規範第 10.5 條與第 11.5 條中對此均有明確記載，可協助確保關鍵系統的存取與變更透明化且獲得妥適記錄。為能有效兼顧資訊安全與法規遵循，FIM 軟體也應當整合 SIEM 解決方案，以提供與其他安全事件間的關連，並保障關鍵資料與系統的安全。

NetIQ Change Guardian 能夠即時偵測重要檔案和系統組態是否遭受未經授權的存取與變更，並發出警告。除了減少資料外洩與內部攻擊的風險之外，本產品還能針對基礎架構中其他重要元件 (例如 Active Directory 與群組規則物件) 的變更，提供「人、事、時、地」的資訊。

本解決方案在搭配傳統 SIEM 解決方案之後，能有效減少收集資訊所需時間，加快決策腳步，減少資料外洩的風險。

若想進一步瞭解如何因應您對檔案完整性監控的需求，請瀏覽 **www.netiq.com**，或是致電當地 NetIQ 業務代表或合作夥伴。

關於 NetIQ

NetIQ 是一家全球 IT 企業軟體公司，客戶的成功是我們永續致力的焦點。客戶與合作夥伴一致選擇 NetIQ，無非是因為本公司能協助他們以符合成本效益的方式，因應資訊保護方面的挑戰，同時管理動態且高度分散的商務應用程式。

本公司的產品組合包括可擴充的自動化解決方案，範圍涵蓋身分識別、資訊安全和治理、IT 作業管理等領域，可以協助各家組織在實體、虛擬和雲端運算環境中，安全地提供、評量及管理運算服務。有了這些解決方案，加上本公司採取以客為尊的務實策略來解決接踵而至的 IT 難題，因此可確保企業組織能夠降低成本、複雜性及風險。

欲進一步瞭解本公司備受業界讚譽的軟體解決方案，請瀏覽 **www.netiq.com**

562-TW1007-002

全球總部

515 Post Oak Boulevard，Suite 1200
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

分公司的完整列表

北美、歐洲、中東、非洲、亞太地區和
拉丁美洲分公司，請瀏覽
www.netiq.com/contacts。