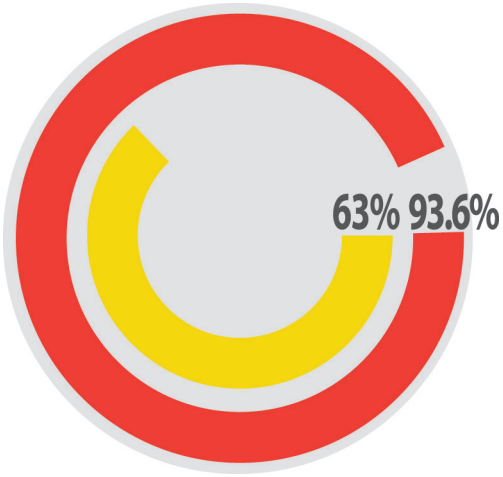
持續不斷的進階威脅：
盜用內部人員的身分證明

您能夠在安全威脅造成傷害前及時將其排除嗎？

在現今的環境中，身分識別與存取管理解決方案已可謂必要配備。企業必須確定員工的身分並授予適當的存取權限，才能維持正常營運。然而，上述論點並未考量到一個關鍵問題：您確定用來存取公司系統的使用者身分證明確實為本人所使用嗎？

大多數的組織都會努力確保各方面皆符合企業安全規則與治理要求。但是這未必代表組織就能獲得妥善的保護。大多數的網路威脅都是遠在修正行動採取之前就已經造成傷害。身分識別的管理十分重要；但是若無法追蹤相關身分的行為，則亦會形成一種安全的錯覺。某些特定的登入身分證明看起來或許並無異樣，某些行為也或許適切如常，但是這些身分證明與行為真的符合業務需求嗎？如果不能就個別身分識別解釋其活動，那麼您的組織可能已經曝露於風險之下。

這種行為追蹤對於受到嚴格管制的產業 (如政府或金融機構) 而言，可能具有較為顯著的意義。這類機構若要持續營運，就必須獲得客戶高度的信賴，讓客戶確信自己的資訊受到妥善保護。也是因為需要公眾的信賴，這類產業才會優先受到管制。但是現在漸漸演變成各種產業的企業都有可能受到攻擊，而攻擊目標也常常出人意表。若不確實掌握使用者利用自己的存取權限進行什麼樣的活動，任何機密資料都有可能曝露於風險之下。



企業是否處於風險之中？

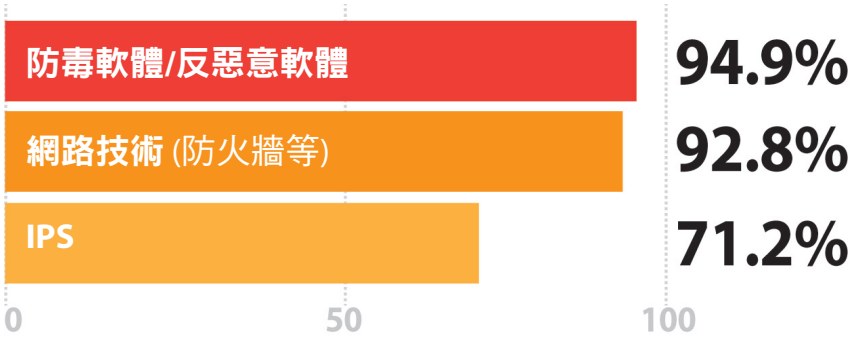
APT 是非常重大的威脅..... **93.6%**
公司被當成目標是遲早的事..... **63%**

ISACA 調查： *全球 1,500 名專業人士*

請問問自己以下有關身分識別與存取解決方案的問題：

- *您有身分識別與存取管理解決方案嗎？(如果沒有，建議您停止閱讀本文，然後趕快去購買一套。)*
- *您能夠監控網路內部使用者活動嗎？*
- *您能夠將活動與個人連結在一起嗎？*
- *您知道什麼人負責什麼活動，及其背後理由嗎？*
- *當使用者行動不符其應有的行為時，您能夠立即採取行動嗎？*

NetIQ



大家是如何處理威脅？

ISACA 調查：*全球 1,500 名專業人士*

癱瘓式威脅與難以察覺的威脅

過去的安全焦點是落在保護重要資料，築起「高牆」將資料圍起；但是現今的網路威脅卻已不再是單純的直線攻擊。「持續不斷的進階威脅」(簡稱 APT) 意指團隊形態的攻擊者，日以繼夜地設法竊取內部人員的身分證明來滲透網路，在不受察覺的情況下持續擷取資料。此類攻擊通常著重於小心翼翼地擴大存取範圍，以便更深入滲透，或進一步入侵其他公司。

在 2009 年，有一位 Twitter 管理員的電子郵件帳戶遭到入侵。通常這不會形成企業規模的問題，但此個人漏洞卻被利用來滲透該名員工的 Google Apps 帳戶。Twitter 當時是以 Google Apps 作為共享機密文件與資訊的管道。Twitter 所面臨的難題就在於這位員工持有已知且受信任的身分識別。存取文件的動作本身並非可疑行為。Twitter 無法在對該活動套用規則，也因此無法確認存取 (與轉寄) 機密文件對於該名使用者而言是否屬適切行為。事實上，Twitter 一開始甚至對漏洞範圍毫無所覺。

Twitter 的安全漏洞對形象的影響反而大於實際傷害，不過這類攻擊確實有越來越常見的傾向。不久前，美國國土安全部也發現了一起組織性的網路入侵案件，主要是透過魚叉式網路釣魚電子郵件來攻擊能源產業。由於沒有資料遭竊或採取惡意行動的證據，因此無法掌握駭客的意圖。但是，這次的攻擊讓攻擊者得以存取重要的控制系統，包括主要天然氣管線的控制系統。這個漏洞與Twitter事件一樣，並未造成災難性的傷害。但是，若這群駭客有意為害，則被動式的分析將無法預防可能造成嚴重後果的問題發生。

事實就是安全威脅的本質已經改變。光透過防火牆保護資訊已經不夠。有太多能夠接觸到機密資訊和系統的間接途徑。不過，在此同時，您也不能直接將所有系統關閉；使用者仍需存取資訊。新的安全典範不僅著重於防止存取，更強調主動監控。該怎麼做才能維護安全，並在造成傷害之前採取預防措施？關鍵就在於找出威脅來源，並採取適當的預防措施。

自動化即時威脅回應

採取預防措施說來容易做來難。重大入侵事件的發生十分迅速，因此您無法仰賴人工作業的方式來及時回應威脅。其中關鍵就在於設置自動化的系統，以便隨時做出回應。

自動化才能實現即時的威脅回應。在理想情況下，您可以設置一套規則，讓系統能夠持續監控各方行為並立即辨識出可疑活動。例如，一般常見的金融交易可能需要接觸到身分識別管理系統、終端使用者終端機以及交易資料庫，才能完成交易與支付款項。身分識別管理系統會驗證使用者的身分。資料庫負責產生記錄資料，SIEM 系統則追蹤使用者在這些應用程式裡執行的每一個動作。但是假設一名員工擁有資料庫的管理員存取權限，而其帳戶遭到入侵，那麼該帳戶就有可能避開既定程序 (即外部客戶必須遵守的程序)，然後進行未經授權的交易，進而竊取金錢。在理想的情況下，系統應能夠辨識出這些動作屬於可疑活動，並自動即時中止交易。

現在有些企業開始採用拉斯維加斯賭場式的安全策略。賭場採取來者不拒的策略，但會全面監控賓客的活動。大多數企業都會想維持一定程度的身分證明檢查，而自動化也能實現類似的概念。您希望能夠保護重要資訊的安全，同時不妨礙使用者活動。規則工具可以讓您建立預期出現的活動，並定義此類活動足以構成通訊協定漏洞的臨界值。這項安全機制雖然透明，但卻十分有效。這種安全策略對於大學或其他具備以下需求的機構可能特別有用：必須進行大量資料共享，但如果出現違反一組定義參數的活動時，仍可中止該活動的進行。

找出並選擇現代安全解決方案

安全威脅已有所改變，組織也必須隨之改變觀念與策略。您必須採取更周全的策略，不僅需注重安全，更要對活動進行控管。在尋找解決方案時，應考慮以下幾個重點。請確認您選擇的解決方案能夠：

1. **連結您的身分識別與存取系統；理想上應能連結您的安全資訊與事件管理解決方案**
2. **讓您制定精細的行為規則**
3. **針對異常或不符業務需求的內部活動發出警告**
4. **以分層、自動化的方式回應潛在威脅。**

隨著安全威脅的演化，您的回應能力也必須有相對的成長，如此才能克服挑戰。就如同向量，您的安全方向與速度必須配合這個逐漸以科技為導向的世界而有所調整，以求跟上世界變遷的腳步。

降低 APT 威脅的關鍵，就在於能否在造成傷害前迅速偵測到並遏止攻擊。NetIQ 能協助您保護重要資訊資產，提供解決方案讓您更清楚掌握使用者活動，以更快的速度辨識出高風險活動，而且還能彙整重要的安全情報。欲知詳情，請造訪 NetIQ 偵測並遏止資料外洩網頁：https://www.netiq.com/solutions/security-management/data-breach-threat-detection.html。

www.netiq.com

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分公司的完整列表，請瀏覽 www.netiq.com/contacts。

追蹤我們的動態：

584-TW0007-001 08/14 DS