SailPoint
The Power of Identity

sailpoint.com

SecurityIQ

非結構化數據的完整存取管理

SailPoint | SecurityIQ

管理對非結構化數據的存取是個日益嚴重的問題。數據資料儲存在檔案伺服器和網路儲存(NAS)設備以及協同入口網站、郵件信箱和雲端資料夾中，在過去幾年呈現指數增長。然而，組織若無容易的方法來追蹤、控制和保護非結構化數據資料，就會面臨不斷增加的安全、法律和監管的風險。

SecurityIQ讓組織能夠集中控管對非結構化數據資料的存取，並對雲端或企業內部所有的系統採用一致性的管理程序、政策和控制。

數據發現和分類

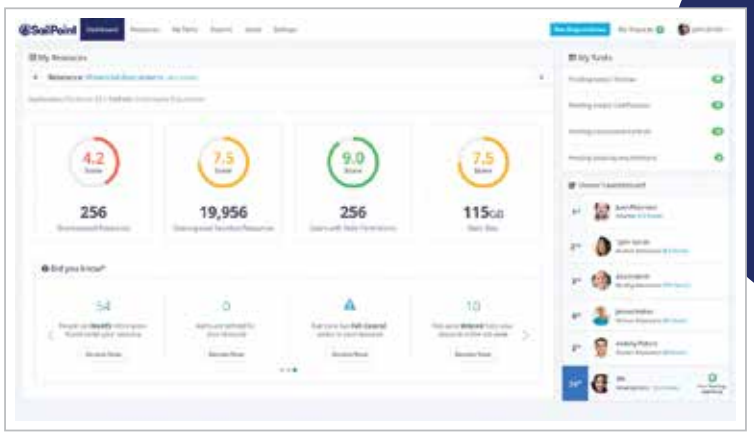
找到敏感數據儲存在何處

在大多數組織中，敏感資料例如財務資料、客戶資料、信用卡資料和個人健康資料可能會儲存在好幾百個不同的地方 — 檔案分享、SharePoint網站、雲端儲存服務和電子郵件資料夾中。SecurityIQ讓組織得以找到敏感資料並將其分類，以便建立有效的控制來管理並保護這些資訊。

授權管理

決定誰可存取敏感數據

非結構化數據的存取可能很難予以視覺化，且若無法清楚知道使用者如何被授權存取，就不可能對存取做好管理和控制。SecurityIQ自動收集和分析有效的授權，橫跨企業內部的視窗檔案伺服器、NAS設備、SharePoint和Exchange、以及雲端入口網站，包括Office 365、Box、Dropbox、MS OneDrive和Google Drive。



讓數據擁有者能夠經由直覺式的儀表板來控制使用者對其數據的存取和使用。

數據活動追蹤

找出誰存取敏感資料及更多相關資訊

可防止安全漏洞和資訊竊取，或當某些事情發生時，組織需要即時對使用者追蹤並了解他們對敏感資料的存取，以及能夠實時回應違規行為，將可能的損害降至最低。SecurityIQ 在受監控的資源上，捕捉所有的使用者事件，並從目錄、IAM系統、HR應用程式和任何其它數據來源收集使用者和設備細節，詳盡描述捕捉到的事件。

完整覆蓋

擴展你的IAM策略

SecurityIQ與SailPoint IAM解決方案分享資訊，提供廣泛對非結構化數據的存取管理。通過使用來自非結構化數據目標的權限數據以擴充來自結構化系統的IAM數據，您的組織因而可以更快速辨識風險、找出合規問題、並作出正確決定以強化控制。

SecurityIQ讓客戶能夠：

- 降低不適當存取的風險
- 改善稽核效能
- 降低營運成本
- 改善 IT人員的生產力

與眾不同，顯而易見。

- SecurityIQ 改善數據安全態勢，讓相關數據擁有者能夠經由直覺的儀表板控制使用者對其數據的存取和使用。
- SecurityIQ 將數據洩漏或違規的風險降至最低，找出敏感數據檔案例如PII,PHI和PCI，並監控對這些檔案的存取動作
- SecurityIQ 統合身份與數據治理政策，針對所有儲存在企業內部及雲端的檔案，集中管理存取作業。

SailPoint | SecurityIQ

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint毫無疑問是身份治理領域中的領導者，為全球企業用戶帶來「身份的強大力量」。SailPoint的開放身份平台給予企業進入新市場的力量，擴大員工作業能量，擁抱新的科技與更快速的創新，並於全球規模內展開競爭力 — 安全且充滿信心。

本公司開創身份治理市場，並提供以雲端為基礎的整合服務，包括合規控制、配置、密碼管理、單一登入和資料存取治理；這一切皆建立於我們相信身份是一個企業運轉的關鍵。

SailPoint的客戶都是全球最大的公司，且涵蓋每一個產業，包括全球前八大銀行、四個前五大健康照護企業、六個前七大產物和意外保險公司、以及前五大製藥公司。

 SP1063-1611