

將身份治理功能延伸到檔案中儲存的資料

許多組織已經採用了身份治理解決方案，藉此保護對應用程式的存取權，但這不是一個完整的策略。當商務使用者建立文件、簡報和報告時，常會從這些應用程式匯出敏感資料，並將其儲存在未受治理的儲存庫中，例如檔案共用 SharePoint 或 Box 中。由於現今的資料外洩和網路威脅早已司空見慣，這種不受保護的敏感資料會帶來嚴重的風險。SailPoint 的 File Access Manager 在企業對包含敏感資訊的檔案存取方式的保護上，引進了創新的作法。

使用全面的身份治理策略保護敏感資料

延伸您的身份治理計畫，以涵蓋儲存在本地端與雲端檔案中的敏感資料，藉此緩解安全性問題、取得即時可視性，並在每個使用者的生命週期中，完整控管其存取權限。

加快遵守規章的速度

透過探索敏感資料所在位置並利用專為符合法規要求而設計的現成原則 (包括 GDPR 和 HIPAA) 來發現重大的合規性差距。自動化存取的檢閱、驗證和審核報告，有助於維護和展示其合規性。

有效地提升企業效率

讓資料負責人有權治理自己的資料，減輕 IT 資源的負擔。利用預先定義的公司原則和身份內容來授與和管理存取權，進而提高企業生產力。

支援雲端就緒

將應用程式和資料移轉至雲端之前，主動解決存取問題並採用正確的存取控制措施。清理權限、識別敏感或過度暴露的資料，並將存取控制措施延伸到儲存在雲端中的資料，以降低風險並支援成功移轉。

將身份治理功能延伸到檔案中儲存的資料

許多組織已經採用了身份治理解決方案，藉此保護對應用程式的存取權，但這不是一個完整的策略。當商務使用者建立文件、簡報和報告時，常會從這些應用程式匯出敏感資料，並將其儲存在未受治理的儲存庫中，例如檔案共用 SharePoint 或 Box 中。由於現今的資料外洩和網路威脅早已司空見慣，這種不受保護的敏感資料會帶來嚴重的風險。SailPoint 的 File Access Manager 在企業對包含敏感資訊的檔案存取方式的保護上，引進了創新的作法。

使用全面的身份治理策略保護敏感資料

延伸您的身份治理計畫，以涵蓋儲存在本地端與雲端檔案中的敏感資料，藉此緩解安全性問題、取得即時可視性，並在每個使用者的生命週期中，完整控管其存取權限。

加快遵守規章的速度

透過探索敏感資料所在位置並利用專為符合法規要求而設計的現成原則 (包括 GDPR 和 HIPAA) 來發現重大的合規性差距。自動化存取的檢閱、驗證和審核報告，有助於維護和展示其合規性。

有效地提升企業效率

讓資料負責人擁有治理自己的資料，減輕 IT 資源的負擔。利用預先定義的公司原則和身份內容來授與和管理存取權，進而提高企業生產力。

支援雲端就緒

將應用程式和資料移轉至雲端之前，主動解決存取問題並採用正確的存取控制措施。清理權限、識別敏感或過度暴露的資料，並將存取控制措施延伸到儲存在雲端中的資料，以降低風險並支援成功移轉。