保護可讓業務發展如虎添翼的資料

IBM Security Guardium 有助於企業進行分析、防護及調整，提供全方位的資料保護

IBM

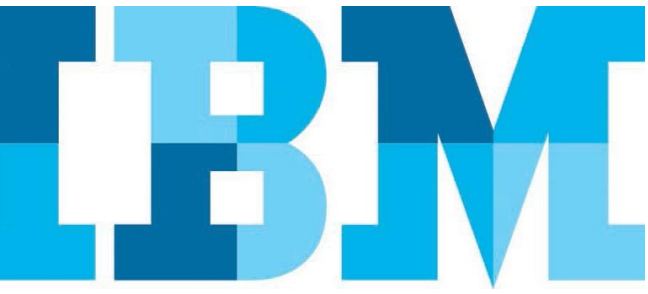
重點特色

- 主動全面保護關鍵資料，橫跨所有種類的平台，包括主要的資料庫、資料倉儲、海量資料平台、雲端環境、檔案系統等
- 自動找出敏感資料、預先察覺風險並採取因應措施，繼而降低整體擁有成本
- 透過加密、遮罩、修訂、活動監控、動態封鎖、警示和隔離等功能，保護敏感資料，抵禦資安威脅
- 利用自動化的資料合規作業取得正確報表，適時提供給適當的人員
- 因應 IT 環境的變化並全程支援資料防護

目前資料外洩安全事件頻傳，造成的影響甚鉅。全球研究指出，企業目前花費在資料缺口的總成本已高達四百萬美元 [1]。此外，若企業組織的商業機密、產品設計與其他智慧財產外洩，也可能導致企業的財務狀況受到嚴重衝擊。由於關鍵的敏感資料實屬業務往來的核心且極富價值，自然成為攻擊者覬覦鎖定的目標。

一般來說，企業組織的資安作業著重「周邊」防禦，以期保護內部重要資訊。不過防毒軟體與防火牆等傳統工具在遇上現今多數來自內部的進階威脅時，通常無法發揮防禦效果。另外，資料的數量會持續增長，也會出現變更及轉移，所以保護資料的方式也必須因時制宜，才能因應資料的變化。越來越多的使用者、應用程式與系統需要即時存取不同類型的敏感資料，將資料存放或複製到資料庫、資料倉儲、檔案共享系統、海量資料平台和雲端環境中。若想持續追蹤有權存取各種分散的動態資料的人員，還有分享資料的人員和分享對象，似乎是難如登天的任務。

IBM® Security Guardium® 專為保護分散四處的關鍵資料而精心設計。這是全面性的資料保護平台，能夠讓資安團隊自動分析整個資料環境中所發生的事件，進而將風險降到最低、保護敏感資料不受內部和外部的威脅，同時協助企業順利因應各種影響資料安全與合規作業的異動。



值得仰賴的全方位資料安全性

Guardium 提供完善的方法，全面保護企業組織的「珍寶」，也就是攸關企業成敗與生存的重要資料。利用 Guardium 的點對點圖像式使用者介面，不論資料狀態為閒置或正在使用中，資安團隊可以找出並降低敏感資料風險。這種整合式的方法還可加以延伸，供一系列結構化資料與未結構化資料儲存庫使用，例如資料庫、資料倉儲、Hadoop、NoSQL、記憶體內部系統、檔案分享系統等。

事實上，Guardium 靈活度十足，可因應各種資料安全與防護需求，無論是基礎合規作業還是全方位的資料防護都不成問題，不僅符合成本效益，也可進一步擴充。這套多層級的解決方案，涵蓋自動化資料威脅分析、動態資料防護和遍及全企業的能見度，足以因應敏感資料環境的異動。

Guardium 使用認知分析與自動化功能，能夠在今日的異質性環境中協助防護重要資料。

分析敏感資料可能面臨的威脅

為了有效進行資料保護作業，企業組織必須確實掌握需要保護的資料，才能徹底防護。Guardium 可讓資安團隊執行下列作業：

- 自動找出敏感資料與授權然後予以分類，同時讓合規風險無所遁形
- 掌握存取資料的人員、察覺異常狀況並防堵資料遺失情形發生
- 快速分析資料使用模式，進而找出風險所在並加以補救
- 利用自動化的進階分析和機器學習技術來支援分析功能，找出不尋常的高風險行為並加以防堵
- 運用特殊威脅偵測分析功能，及早察覺並防堵安全漏洞，例如察覺 SQL 資料隱碼攻擊或惡意的預存程序，並且發出警告
- 提供儀表板，有助於主要相關人員檢視長期的資料安全性與/或合規狀態和進度，進一步瞭解指定方案如何提升業務價值，同時掌握待補全的缺口

Guardium 可協助資安團隊利用方便好用的圖形使用者介面，自動找出敏感資料並予以分類。資安人員可透過一系列的步驟，找出所有內含敏感資訊的資料來源（包括尚未編錄的資料庫），然後使用可自訂的分類標籤與授權管理功能，自動施行安全政策。資安人員也可將敏感資料搜尋作業納入排程並定期執行，藉此防堵有問題的伺服器，確保不會遺漏任何關鍵資訊。

為協助執行政策並保護敏感資料，Guardium 可持續即時監控存取（或試圖存取）敏感資料的人員。Guardium 優於傳統資料監控模式的一點，就是具備智慧獨具的極端值偵測能力，可依據行為變化來分析及掌握風險。Guardium 採用進階機器學習演算法，可根據詳細的情境式資訊來偵測異常資料存取行為，全面掌握每次資料存取的「人、事、時、地、物」。Guardium 也能透過適應性學習流程，針對新出現的一般活動模式，與系統長期累積的新活動進行比較。直覺式的認知型使用者介面有助於精準找出異常之處，方便管理員深入調查根本原因。

除了深入探查功能外，Guardium 還可讓資安人員在介面中快速搜尋稽核報表與其他項目，也可以針對資料本身，迅速在全企業進行搜尋。使用者無須瞭解基礎的拓撲、彙總或負載平衡配置。無論著重的是特定資料來源、使用者或日期，搜尋要求都可協助從特定資料存取活動擷取洞察。新的調查儀表板也有助於找出資料的固定模式、異常狀況與關係，透過最佳做法預先設定檢視方式，縮小範圍。Guardium 也提供 Connection Profiling 工具，可回報所有企圖存取特定資料來源的連線。

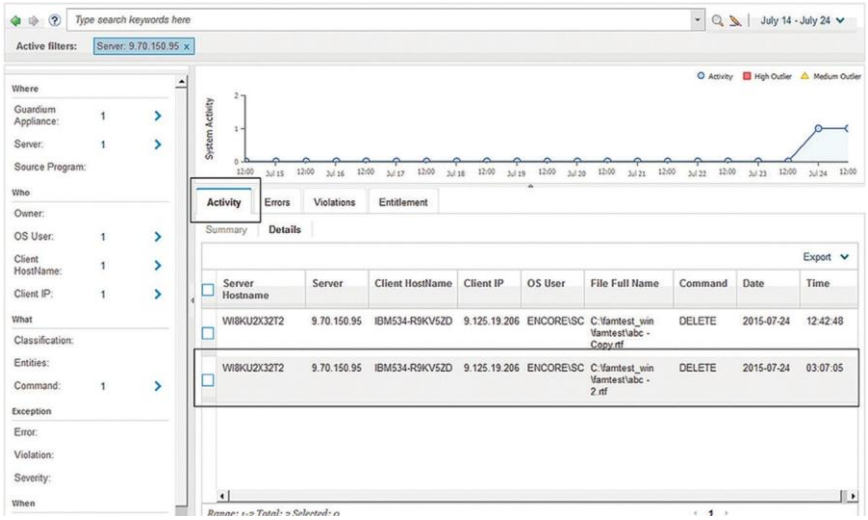
保護敏感資料

敏感資料所面臨的威脅不斷攀升，合規授權需求也持續增加，這兩項議題讓企業組織不得不重新思考自身的資料防護策略。Guardium 可讓資安團隊執行下列作業：

- 運用自動化資料合規與豐富的稽核功能，形成保護企業免受財務風險的最佳屏障
- 透過加密、遮罩、修訂、動態封鎖、警示和隔離等功能，管控關鍵資料
- 運用即時活動監控與封鎖功能，協助避免來自內部和外部的非法資料與檔案存取

Guardium 提供安全且無法竄改的稽核紀錄，可協助企業掌握及審查所有敏感資料的流量，連具備權限的使用者在本機存取的情況也包括在內。事實上，Guardium 的單一集中標準化稽核儲存庫，可提供遍及全企業的合規通報、效能優化、調查與鑑識功能。企業組織可將整個資料合規稽核流程自動化，包括將報表分派給監管團隊、簽名核准、向上呈報等，只需提供已預先設定妥當，支援 Sarbanes-Oxley 法案（SOX）、支付卡產業資料安全標準（PCI DSS）以及資料隱私的報表即可。

Guardium 提供了簡便的圖形介面，能夠找出智慧演算法偵測到的異常狀況並加以因應。



Guardium 的檔案活動監控功能，能讓企業組織針對文件資料偵測與封鎖相關的可疑活動，即使操作人員是具備權限的使用者也不例外。

此外，Guardium 還可讓資安團隊透過檔案式加密、資料庫、海量資料安全漏洞評估、靜態資料遮罩和修訂等功能，由內而外保護敏感性資料，抵禦資安威脅。Guardium 也同時支援動態即時資料遮罩和加密，還能夠封鎖、發送通知與隔離可疑的使用者。事實上，Guardium 能限制不肖份子存取大多數來源的敏感資料，包括雲端環境、海量資料平台與檔案系統等。

Guardium 也能持續監控所有敏感資料的活動狀態，例如即時監控檔案系統存取情形，藉此協助加強職責分工。如此一來，企業組織就能針對具備權限的使用者，偵測、記錄與封鎖對方未經授權的可疑活動。舉例來說，若有人大量複製敏感檔案或目錄，或有特定的系統管理員突然大量存取檔案，Guardium 都可以偵測到這類活動；此外，Guardium 也可以針對不當存取發出警告、封鎖最敏感文件的存取權限，以及為所有活動產生客製化報表。Guardium 還能協助找出資料庫與海量資料基礎架構的曝顯度，確保資料基礎堅若磐石。

應變能力

資料基礎架構持續轉變擴增，因此要能夠持續因應瞬息萬變且不斷出現的安全性缺口，不僅極具挑戰也所費不貲。有了 Guardium，企業組織便能：

- 同時支援傳統與顛覆性的資料技術，例如 Hadoop、NoSQL 與雲端技術
- 從法令遵循合規作業乃至於全方位的資料保護，輕鬆擴充資料防護架構
- 在整個資料環境中，採用可以自動進行負載平衡的單一資料防護基礎架構，進而降低成本及改善作業成效

Guardium 讓企業組織能因應資料環境內的異動，擴充資料防護功能來配合新的使用者、平台與資料類型需求，同時還能整併 IT 運作方式，藉由自動化、集中化與整合，提供可簡化資料安全管理作業的平台。其中也包括美國國家通訊局 (DISA) 授權作業 (ATO) 等立即可用的憑證，或歐盟一般資料保護規範 (GDPR) 等重大法規專用的合規加速器，方便使用者使用。平台本身的重心包括支援傳統型資料庫、雲端環境、Hadoop 式系統、NoSQL、記憶體內部系統與檔案系統。Guardium 提供靈活的控管功能，可針對特定的合規需求進行部署，也可輕鬆擴充，隨著業務需求成長提供額外防護。

Guardium 與單點解決方案不同，能夠支援其他領先業界的安全解決方案、漏洞標準、應用程式和更多異質性整合。Guardium 也提供了最無與倫比的整合方式，能夠搭配 IBM QRadar® SIEM 等 IBM Security 解決方案，提供主動式資料防護。Guardium 可將事件與資料庫搜索/分類資訊發送至 QRadar SIEM，藉此找出更具效益的威脅活動關聯性。此外，Guardium 也可接收 QRadar SIEM 發送的狀態與警示通知，有助於抵禦不肖 IP 來源、不肖使用者與新的安全漏洞，不論威脅來自應用程式、作業系統或其他資料來源都無一遺漏。

例如，Guardium 與 QRadar 相互整合，協助企業組織防範經由應用程式發動的潛在攻擊、偵測 SQL 資料隱碼這類資料庫攻擊，並在資料遭擷取前加以封鎖，同時在應用程式層級找出安全漏洞，進行虛擬修補作業。

Guardium 能為各行各業帶來價值

- **某家大型保險公司**現在只靠一名全職員工，便能管理將近 1,000 個資料庫。
- **某家大型公用事業公司**在一年內達成投資報酬率為 55% 的目標，確保 450 萬個帳號符合 SOX 與 PCI 規範。
- **某家跨足全球的銀行**可監控五千個以上的資料來源，包括即時海量資料交易，同時絲毫不影響關鍵應用程式的效能。
- **某家國際電信公司**現在可以集中監控並即時因應分散在全球 16 座資料中心內、數千個資料庫的資料存取活動。
- **某家汽車製造商**可監控及稽核 500 個正式系統資料庫，除了提升安全性外，還可減少 90 %的資安人員需求。

為何選擇 IBM？

深受全球企業組織信賴的 IBM Security 解決方案能提供進階資料防護。IBM 技術經過實證，能讓組織有效保護關鍵資源，隔絕最新安全威脅。面對新型威脅的崛起，IBM 能運用完整的產品服務組合以及事業夥伴解決方案，幫助組織建置核心安全基礎架構。

IBM 具備在全球提供服務的豐富專業經驗，尤其是合規需求特別嚴謹的產業，例如政府部門、健康照護與金融服務業。作為戰略合作夥伴，IBM 能夠讓企業降低資安漏洞並為複雜的 IT 環境妥善管理風險。

更多資訊

若要獲得 IBM Security Guardium 的更多資訊，請聯絡 0800-016-888 按 1、IBM 業務代表或 IBM 事業夥伴。

關於 IBM Security 解決方案

IBM Security 提供最先進的整合式套裝產品，包含企業級安全性產品與服務。享譽全球的 IBM X-Force® 研發團隊提供此套裝產品的安全性情報協助企業組織全面性保護其員工、基礎架構、資料與應用程式，交付身分與存取、管理、資料庫安全、應用程式開發、風險管理、端點管理以及網路安全性等解決方案。這些解決方案可以協助企業組織有效管理風險，並針對行動、雲端、社群媒體與其他企業級商業架構導入整合式安全性措施。IBM 擁有全球最多元的安全性開發與交付組織，在 130 國家每天監控 150 億安全性事件，並具備 3,000 多個安全性專利。

台灣國際商業機器股份有限公司

台北市 110 松仁路 7 號 3 樓

2017 年 7 月

1 “2016 Cost of Data Breach Study: Global Analysis,” *Ponemon Institute*, June 2016.**ibm.com**/security/data-breach/