IBM Security Guardium Vulnerability Assessment

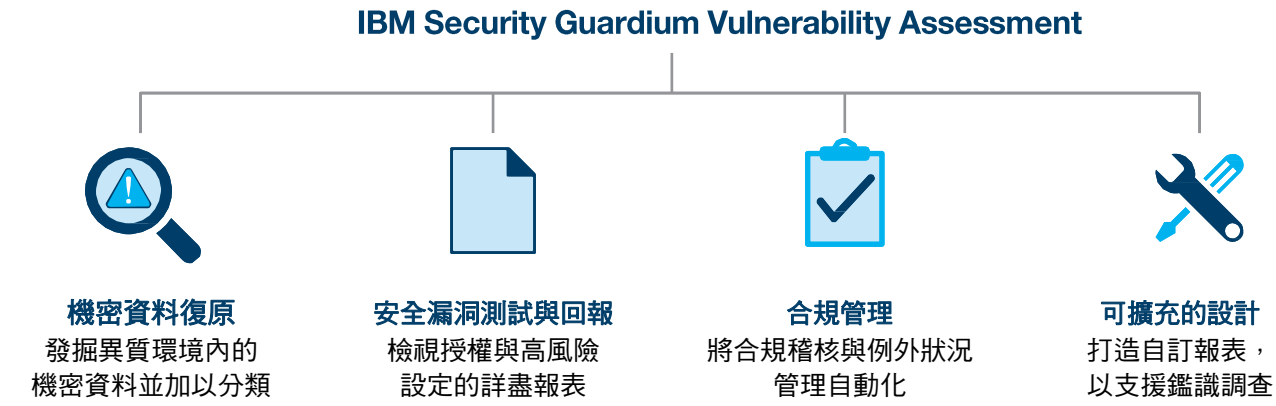
掃描資料環境，以偵測安全漏洞並提供補救建議措施

重點特色

- 提供可擴充平台，為客戶資料儲存庫的安全嚴格把關，同時管理合規要求以符合最新的安全法規
- 為每項資料來源類別選用特定的測試與自訂選項，以強化資安最佳實務做法
- 運用彈性報表，取得修復每項資料來源安全漏洞的建議處理方式，藉此解決對資料的威脅並簡化安全作業

IBM Security Guardium Vulnerability Assessment 能定期掃描目標系統，偵測安全漏洞，以鞏固資料基礎架構。資料基礎架構十分彈性，會定期更新帳號、設定與修補程式。多數企業組織由於缺乏集中控管或熟練的資源，因此無法協助公司以有系統的方式檢視異動，藉此判定這些變更是否造成安全漏洞。

Guardium Vulnerability Assessment 的重要性不可忽視，能找出資料庫、資料倉儲與海量資料環境內的資安威脅與安全漏洞，以免入侵系統的駭客得手並取得存取權限與機密資料。Guardium Vulnerability Assessment 可提出具體的建議措施，以鞏固系統安全性，並消弭不安全的資料儲存庫設定、修補程式缺漏、密碼強度過低與其他漏洞所導致的巨大風險。Guardium Vulnerability Assessment 會提供結果概覽，助您掌握系統安全性的整體情況，並在詳盡的細項報表內提供具體改善建議。Guardium Vulnerability Assessment 這項單一服務可支援多個資料平台，不僅可擴充性十足，更能降低整體擁有成本，提昇安全並透過一系列核心功能來支援合規要求。這項服務涵蓋上述所有功能。



Guardium Vulnerability Assessment 提供多項核心功能，可助您分析風險、將合規作業自動化，並鞏固您的資料環境。

精簡管理

企業組織不具備在資料層控管安全漏洞的時間與資源。檢查安全漏洞的人工作業變得耗時無趣，而這對資安作業而言，不僅風險高且容易出錯。隨著業務不斷成長，需要顧及安全性的專案也越來越多，您需要更精簡的安全性解決方案。在充斥海量資料的現代，不只資料量暴增，資料的類別與產生速度也與日俱增，因此資安策略必須最佳化且透明化，模稜兩可且更加複雜的策略則行不通。

Guardium Vulnerability Assessment 的首要之務是協助企業組織精簡資安管理，免去修改資料來源、網路或應用程式的作業。資安管理功能包括：

- **自動化更新報表與政策，以因應 IT 環境的變遷與資安事件：**橫跨異質環境，盡可能擴大資安防護的範圍。只要按一下滑鼠，就能同時更新所有分組、策略、測試與其他設定參數，以因應不斷演進的資料基礎架構與相關資安威脅。
- **單一管理主控台：**透過單一網頁式主控台集中控管，建立多樣化資料來源的評估結果。評估結果可透過單一網頁式主控台進行修改、新增或刪除。

- **資料庫探索與資料分類：**探索資料資產並將機密資料分類。可設定探索流程，視排程或需求來探測特定的網路區段。待辨識出相關實例後，系統便會檢查內容，以進行機密資料的辨識與分類。
- **管理進階使用者/角色（職責分工）：**區分資安管理與資料管理。Guardium Vulnerability Assessment 的管理與設定等所有作業，皆須接受稽核以進行合規控管。資安專業人員不需 IT 人員支援也能產出報表，並透過角色存取控管（包括階層式控管）好讓管理員執行存取權限。
- **內建合規工作流程（審核、提報高層和簽署認可）：**支援《沙賓法案》(SOX)、《支付卡產業資料安全標準》(PCI DSS) 以及《健康保險隱私及責任法案》(HIPAA) 等規範。簡單易用的圖形使用者介面，有助於建立各式各樣的流程，以符合待辦任務與相關人員的獨特需求。支援多種稽核任務，包括檢查自動產生的安全漏洞評估結果、資產探索與資料分類。支援的匯出報表格式包括 PDF、CSV、CEF、Syslog、SCAP 與 AXIS，也可自訂 schema（架構），以利整合安全資訊與事件管理 (SIEM) 解決方案，或是提供商務智慧報表。
- **應變式排程與多資料庫報表整合：**安全漏洞測試的整個流程中，每項資源需依照狀態採用不同處理方式。有了應變式排程，系統就可暫緩執行幾項非必要的失效測試，直到安全漏洞修復為止。資料來源亦可按報表用途分類。

效能

業務進展迅速，而客戶存取資料的需求更是分秒不停、全年無休。因此，資料庫、交易應用程式、分析平台以及與日俱增的海量資料應用程式等 IT 環境，無論在可用性、效能與反應靈敏度各方面，都須符合日益嚴苛的服務等級協定。必須著手處理合規要求，並在不影響效能的前提下，落實資安策略。導入 Guardium Vulnerability Assessment 即可採用下列關鍵功能，將效能影響降至最低：

- **快速評估**：只要短短數分鐘，就能完成安全漏洞評估測試。
- **資料庫流量篩選**：避免不必要的資料庫稽核流量，把對正式環境資料庫效能的影響降至最低。
- **支援 64 位元架構**：採用 64 位元可擴充式設備平台，可隨建置規模擴充，並提供足夠處理能力，藉此處理成千上萬筆資料來源的流量分析。

整合

企業組織多半都備有一些安全性解決方案，例如 SIEM 或應用程式層面的存取權限控管。然而，現有的安全性解決方案幾乎都無法為資料來源基礎架構的安全漏洞提供深入洞察。而 Guardium Vulnerability Assessment 在提供深入洞察時，還能與 IBM Security QRadar® 或 HP ArcSight 等現有的安全性解決方案完美整合。此外，Guardium Vulnerability Assessment 這項方案可隨加隨用並附加至現有 IT 系統的整合模型，例如資料管理、工單管理與封存解決方案。這是為了彌補現有 IT 方案的不足之處，並用下列方式維護您的系統安全：

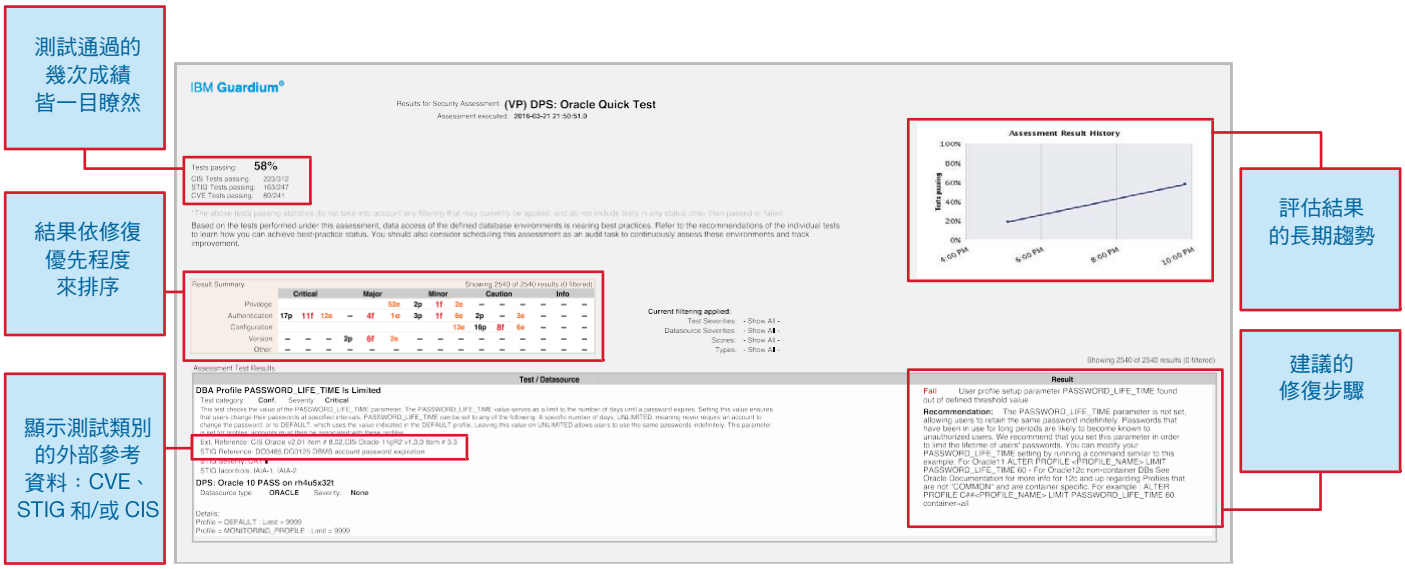
- **整合 IT 作業：**搭配內建且可立即使用的支援功能，便可利用現有的資料管理環境，包括 Oracle、IBM DB2®、IBM DB2 on z/OS®、IBM DB2 on iSeries®、Sybase、Microsoft SQL Server、IBM Informix®、mySQL、Teradata、Aster DB、IBM PureSystems®、PostgreSQL、SAP HANA 和 MongoDB。
- **與安全系統和標準整合：**自動化因應變動。資料庫與應用程式的使用者、群組、角色與身分驗證皆可從 Lightweight Directory Access Protocol (LDAP)、Radius 和 Microsoft Active Directory 等來源自動更新。您可以自動處理任何員工或使用者的異動，無須不斷自行修改這些變更，同時確保符合政策和報告的完整性。儘管 IT 環境不斷變遷，使用群組仍有助於維護資安策略，同時也能建立白名單與黑名單。此外，還可將所有稽核資訊傳送至 QRadar 等 SIEM 資安事件管理解決方案。Guardium 整合 IBM Security zSecure™ Audit 之後，就能夠在 z/OS 專用的 DB2 上，辨識出能存取機密資料的有效授權。

可擴充性

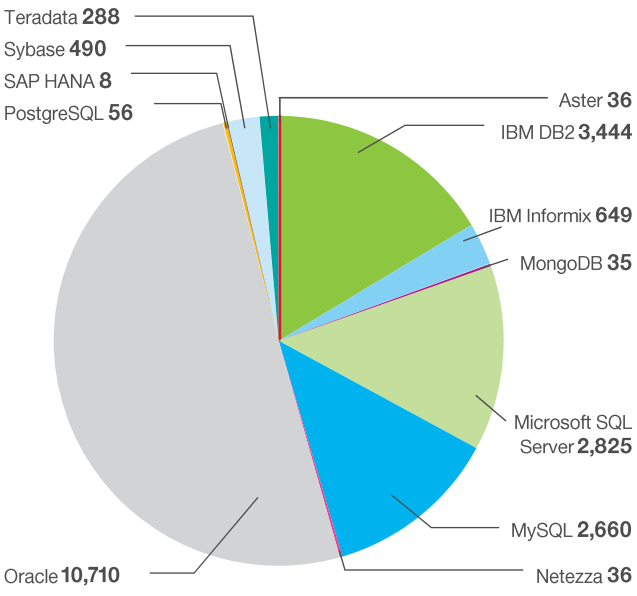
對資料環境而言，資安與合規管理儼然成為一大挑戰：不僅網路攻擊率不斷攀升，環境的複雜程度也急遽增高。業務環境快速變化，合併、外包、勞動力調整和加速業務自動化等因素，帶動了資料儲存庫數量遽增，而且橫越實際地理位置與企業組織的疆界。礙於目前環境的資源有限、環境管理更形複雜以及工作負載持續攀升，企業組織非常希望增加資料庫安全性和合規性作業的自動化。Guardium Vulnerability Assessment 能從單一資料來源擴充至上萬個資料來源，完全不會造成作業中斷，橫跨多座資料中心與多處地理位置也沒問題。自動化功能包括：

- **透過 GuardAPI 支援批次作業：**促進所有與 Guardium Vulnerability Assessment 整合的 IT 作業流程。GuardAPI 是連接 Guardium 的腳本式命令列介面（CLI），允許遠端執行操作。
- **彙總：**合併多個來源的安全漏洞評估報表，橫跨異質平台，為企業提供全面報表。

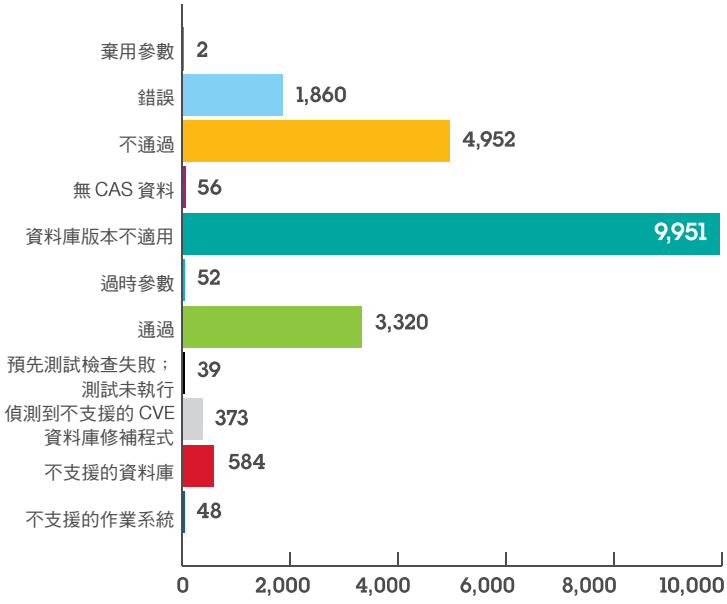
在客戶端環境測試 IBM Security Guardium Vulnerability Assessment



各平台的評估報表數*



掃描結果的評估概覽*



* 圖表會顯示特定期間內在客戶環境進行測試所取得的各平台評估結果數與掃描結果的評估概覽。

Guardium Vulnerability Assessment 提供掃描結果的詳盡報告，包括修復用的建議步驟。評估在眾多平台上執行，可辨識出錯誤的設定、不支援的資料庫修補程式等眾多安全性漏洞。

降低風險

風險代表指定的行動或活動（包括選擇不執行的行動）會導致機密資料暴露的可能性。必須率先採取應對措施，先發制人，以防堵資安威脅，避免因內外安全漏洞而導致損害、風險、資料遺失或其他負面影響的可能性。Guardium Vulnerability Assessment 透過及早發現和修復資料來源漏洞，來降低風險。為支援合規要求，Guardium Vulnerability Assessment 也提供安全漏洞報表與警示功能。部分關鍵風險控管功能如下：

- **自訂報表產生器與深入查詢功能：**使用 Guardium Vulnerability Assessment 統計報表，產生資安健康狀況卡和儀表板式報表。針對每項主要測試類別，監控概覽內的筆數（執行測試總數、成功筆數與失敗筆數）：網路安全中心 (Center for Internet Security，CIS)、資料庫安全技術建置指南 (Security Technical Implementation Guide，STIG) 與常見安全漏洞事件 (Common Vulnerability Event，CVE)。快速找到感興趣的測試，無需事先篩選數不清的報表。
- **最佳實務建議（預先定義的報表與警示功能）：**提出具體的行動規劃建議，以鞏固資料資產的安全性，並在發現安全漏洞時即時收到系統警示。您也可以定義自訂測試，並安排自動化稽核任務，結合掃描功能、報表分配、電子簽署認可與提報上級等功能。
- **安全漏洞評估：**掃描資料基礎架構是否存在安全漏洞，以辨識是否發生缺少修補程式、密碼強度過低、設定錯誤的權限與預設供應商帳號等資安風險。簡化大規模環境的部署作業，因為可以載入多項資料來源（資料庫名稱、類型、伺服器 IP、連接埠和角色）並自動連結至評估功能。評估結果將分類為多種類別，如權限等級、身分驗證、版本、行為、檔案權限與設定。使用即時資料與歷史資料，提供目前安全狀態的評估結果。
- **訂閱資料庫防護知識庫：**採用最新的安全漏洞標準，自動運用資料漏洞修復更新。此服務提供軟體修復程式等級、版本等級、易受攻擊的物件、敏感物件（具有 SOX 的資料庫表格、可辨識的個人資訊、或 PCI DSS 資料）、儲存程序、行政管理程式、指令等多種項目。使用多種來源以辨識此項資訊，包括 IBM 內部研究報告，與其他供應商的關係，以及 CVE 等跨產業協同合作。搭配企業應用程式內（SAP、Oracle E-Business Suite、PeopleSoft 等）常見的安全漏洞、最佳實務資安策略和機密資料表的最新資訊，主動更新 Guardium Vulnerability Assessment，便可省下許多時間心力，而無須耗費在不斷嘗試找出新漏洞。
- **設定稽核系統 (CAS)：**評估作業系統和資料儲存庫設定的安全漏洞，並在設定異動時發出警示。追踪資料庫引擎範圍之外且可能危及資料環境安全性的所有異動，包括資料庫設定檔案（例如 SQLNET.ORA 與 NAMES.ORA）、環境與和登錄變數，shell 腳本、作業系統檔案與可執行檔。即時掌握各種資料庫系統的變化是一項挑戰；因為資料庫架構、文件和發佈時程表各有獨特之處。Guardium Vulnerability Assessment 的追蹤功能完全自動化。
- **修復安全漏洞的最佳實務建議：**依據上百種全面預先設定測試，來強化資料庫安全，包括透過 CIS 和 STIG 而開發的內建最佳實務做法以及 SCAP 的支援。

為何選擇 Guardium？

Guardium 屬於 IBM Security Systems Framework 和 IBM Data Security Privacy Platform 的一部分。資料安全和隱私平台提供一站式資料保護功能，可為您找出環境內最重要的資料，並進行分析、保護、整合和管理。Guardium 提供打造資料保護碉堡所需的一磚一瓦：從滿足合規需求到全面的資料防護。模組化的產品組合為使用者提供極大彈性，可自由選擇開始建置的地點，並結合不同資安軟體或搭配其他供應商的元件，也可選擇同時部署多項產品，以加速資安防護並提昇價值。對資訊密集型專案而言，資安平台是企業等級的扎實基礎，為企業組織提供必要效能、可擴充性、可靠度並提升速度，才能將難以對付的問題簡化，並加快向業務交付可靠資訊的腳步。

無論資料存放在海量資料平台、資料庫或檔案系統，IBM Security Guardium 這個全方位資安平台都可協助資安團隊持續提供防護並管理各式各樣的機密資料。

為何選擇 IBM？

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。此產品組合由聞名全球的 IBM X-Force® 研發支援，提供安全情報，協助企業全面保護員工、基礎設施、資料和應用程式，提供身份和存取權限管理、資料庫安全、應用程式開發、風險管理、端點管理、網路安全等多項解決方案。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 致力於全球最深入的資安研究、開發和交付，每天在全球 130 多個國家/地區監控 150 億起資安事件，並擁有 3,000 多項資安專利。

更多資訊

如需進一步瞭解 IBM Security Guardium Vulnerability Assessment，請聯絡您的 IBM 業務代表或「IBM 事業夥伴」，您亦可造訪下列網站：**ibm.com**/guardium，或聯繫 0800-016-888

IBM 全球融資事業部提供數個付款方式，讓您可以購買 IBM 技術來滿足您的業務成長。我們提供完整的 IT 產品與服務生命週期，從購買到產品處理面面俱到。
如需更多資訊，請造訪下列網站：**ibm.com**/financing

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

2016 年 4 月

本文件中提及的內容在發表當時保持最新狀態，IBM 隨時可能變更其內容。IBM 事業夥伴會提供各自的定價，而該定價會因不同狀況而異。

本文所討論之效能資料皆由特定操作條件下獲得。實際結果可能不同。使用者有義務自行評估和確定任何其他產品或程式和 IBM 產品及程式間的運作。

此文件所提供的資訊係依「現況」提供本出版品，不提供任何明示或默示之保證，包括不提供任何可商用性及特定目的之適用性的保證，也不提供不違反規定的保證或條款。IBM 產品依相關合約條款之規定提供保證。

客戶需自行負責確保遵循法令規定。IBM 並不提供任何法律建議，亦不表示或保證其服務或產品將確保客戶遵循任何法規。

任何關於 IBM 未來方向及發展的陳述可能有所變更或撤銷而不另行通知，僅代表未來目標。

愛護環境，敬請回收

良好安全工作聲明：IT 系統的安全性包括保護系統與資訊，藉由透過預防、偵測及應變所有企業內外不當的存取而達成。不當的存取可能導致資訊被篡改、破壞、盜用或濫用，或可能造成系統受損或誤用，包括被用來攻擊其他系統。沒有任何 IT 系統或產品是絕對安全的，也沒有任何產品、服務或安全措施在防範濫用或不當存取上是絕對有效的。IBM 系統、產品和服務的設計絕對合乎法律規範，並擁有全面的安全性方案，而這必定需要額外的操作過程，也可能需利用其他系統、產品或服務來達到最高效率化。IBM 不保證系統、產品或服務能免於或讓您的企業免於任何惡意或非法行為的影響。

WGD03074-USEN-01