IBM Guardium 7

全方位管理「資料庫安全」和「法規遵循之生命週期」

全球1000多家組織肯定 IBM 子公司 Guardium 超越其他技術供應商，可保護關鍵的企業資料安全。Guardium 提供了最簡單、最強大的解決方案，保障企業系統中的財務和 ERP 資訊、客戶和員工資料，以及智慧財產的安全。

我們的企業安全平台，能夠阻止內部專用權使用者和潛在攻擊者所做的未授權或可疑活動，還能監控企業應用（例如 Oracle E-Business Suite、PeopleSoft、SAP 以及內部系統）終端使用者的潛在詐欺行為。

同時，我們的解決方案借助可擴充的多層次架構，最佳化作業效率，自動化和集中完整應用和資料庫基礎設施中的法規遵循控制。

此解決方案不但功能強大，其實用性也同樣引人注目，對效能幾乎不會造成影響。您不需更改資料庫，也不用依賴本機資料庫日誌與公用稽核程式。

即時資料庫安全保護和監控

獨一無二的 Guardium 7 解[illegible]化、調查和法律取證，後端資料儲存和工作流程自動化系統，全面管理資料庫安全和法規遵循的生命週期，協助您：

- 找出和分類企業資料庫中的機密資訊。
- 評估資料庫漏洞和配置缺陷。
- 執行建議的更改後鎖定配置。
- 利用支援「職權分立」的安全、防竄改的稽核追蹤，提供所有資料庫交易活動全面的可見度和精細控制（跨越所有平台和協定）。
- 監控機密資料存取、專用權使用者行為、變更控制、應用使用者活動和安全性異常（例如登錄失敗），並執行策略。
- 使用針對 SOX、PCI DSS 和資料隱私進行預先配置的報告，自動化完整遵循性稽核流程，包括向監督團隊分發報告、報告簽署和升級。
- 建立單一、集中的稽核資料儲存庫。
- 從保護單一資料庫，擴展為輕鬆保護全球各資料中心的數千資料庫。

尋找與分類

自動找出、分類和保護機密資訊

組織建立和維護的數位資訊日益增加，越來越難以定位和分類機密資訊。

在經歷過合併的組織，或是原始開發人員進入公司前就存在舊系統的環境，這尤其具有挑戰性。即使一切順利，（新業務所需的）應用和資料庫結構會不斷變化，也很容易使靜態安全策略失去效用，並使機密資料定位不明且失去保護。

組織特別難以處理以下事務：

- 明確規劃包含機密資訊的所有資料庫伺服器，以及理解所有源頭（業務應用、批次處理流程、臨機查詢、應用開發人員、管理員等）如何存取資料。
- 在不知道資訊機密性的情況下，保護資訊和控管風險。
- 在不清楚哪些資訊受特定法規管轄的情況下確保遵循性。

借助 Guardium，您可以使用資料庫自動發現和資訊分類功能，找出機密資料儲存於何處，然後使用可自行定義的分類標籤，自動執行適用於特定機密物件類別的安全策略，確保機密資訊僅供獲得授權的使用者查詢及更改。

您也可以定期尋找機密資料，預防惡意伺服器的介入，確保不會「遺忘」任何關鍵資訊。

評估與加強保護

漏洞、配置和行爲評估

Guardium 的資料庫安全評估功能，可對整個資料庫基礎設施執行漏洞掃描，並使用即時和歷史資料，持續評估資料庫的安全狀態。

Guardium 提供全方位的預先配置測試庫，依據業界最佳實務與特定的平台漏洞，透過 Guardium 的訂閱服務定期更新。您也可以針對特定需求自行定義測試。此外評估模組還可標記法規遵循漏洞，例如未經授權的存取（為實現 SOX 和 PCI DSS 遵循性而保留的 Oracle EBS 和 SAP 表格）。

評估分為兩個主要類別：

- 漏洞和配置測試用於檢查錯誤的修補程式、錯誤配置的專用權和預設帳戶。
- 行為測試可即時監控所有資料庫流量，根據存取或操作資料庫的方式（例如太多次登錄失敗、使用者端執行管理命令或下班後登錄）來識別漏洞。

評估模組除了產生逐層分析的詳細報告，還可產生使用權重指標（基於最佳實務）的安全健康分數卡，並建議具體的操作計畫來加強資料庫安全。

配置鎖定和變更追蹤

一旦完成了由漏洞評估功能生成的建議操作，您就可以建立安全的配置基準。使用 Guardium 的配置稽核系統 (CAS)，您可以監控此基準的任何更改，確保沒有超出您授權的變更控制策略和流程。

監控與策略執行

監控和執行資料庫安全和變更控制策略

Guardium 提供精細即時的策略來管理資料庫帳戶的專用權，進而阻止未授權的可疑行為，以及來自惡意使用者或外部人員的攻擊。您也可以識別透過單個多層次應用（例如Oracle EBS、PeopleSoft、Siebel、SAP，以及 IBM WebSphere、Oracle WebLogic 和 Oracle AS 的自定義系統）通用服務帳戶，對資料庫進行未授權存取的應用使用者。

該解決方案可由資訊安全人員管理，無需資料庫管理員 (DBA) 的干預。您還可以定義精細的存取策略，根據 OS 登錄、IP 或 MAC 位址、來源應用程式、時間區段、網路協定和 SQL 命令的類型，限制特定表單的存取。

對所有資料庫流量持續進行脈絡分析

Guardium持 續即時地監控所有資料庫操作，使用正在申請專利的語言分析功能，根據詳細的脈絡資訊，檢測未經授權的操作。此類資訊包括各 SQL 操作的「物件、任務、地點、時間和方法」。此一獨特的方法可將錯誤降到最低，提供前所未有的控制，不同於僅尋找預先定義的樣式或特徵的傳統方法。

執行基準測試，檢測異常行爲並自動化策略定義

透過建立基準測試，以及識別正常業務流程和可能的異常活動，系統會自動建議您可以用於防禦 SQL 隱碼等攻擊的策略。您可透過直觀的下拉功能表，輕鬆增加自定義策略。

主動、即時的安全措施

Guardium 提供即時控制項，可主動回應未授權或異常的行為。策略操作可以包括即時安全警報 (SMTP、SNMP、Syslog)，封鎖（透過 TCP 重設或內部的資料防火牆技術）；支援完整日誌，以及自定義操作，例如自動帳戶鎖定、VPN 埠關閉和與周邊 IDS/IPS 系統協調。

追蹤與解決安全事故

法規遵循要求組織證明所有事件都能及時記錄、分析和解決，並呈報管理階層。Guardium 提供業務使用者介面和工作流程自動化機制來解決安全事件，並提供圖形儀表板來追蹤關鍵指標，例如已公開的事件數量、嚴重級別和事件公開的時間長度。

稽核與報告

擷取詳細的稽核追蹤

Guardium 為所有資料庫活動建立連貫、精細的追蹤，以即時的脈絡分析和過濾，實現主動控制，並產生稽核人員所需的特定資訊。

報告詳細記載所有資料庫活動，以證明法規遵循性，包括登錄失敗、專用權提升、模式變更、下班後或從未經授權的應用進行存取，以及機密表格的存取等。

例如，系統會監控所有以下事項：

- 安全異常，例如 SQL 錯誤和登錄失敗。
- DDL 命令，例如更改資料庫結構的建立/棄用/更改表格操作。資料庫結構對於 SOX 等資料治理法規尤其重要。
- SELECT查詢。此類查詢對於 PCI DSS 等資料隱私法規尤其重要。
- DML命令 (Insert、Update、Delete)，包括連結變數。
- 控制帳戶、角色和許可權的DCL命令 (GRANT、REVOKE)。
- DBMS平台支援的程式語言，例如 PL/SQL (Oracle) 和 SQL/PL (IBM)。
- 資料庫執行的 XML。

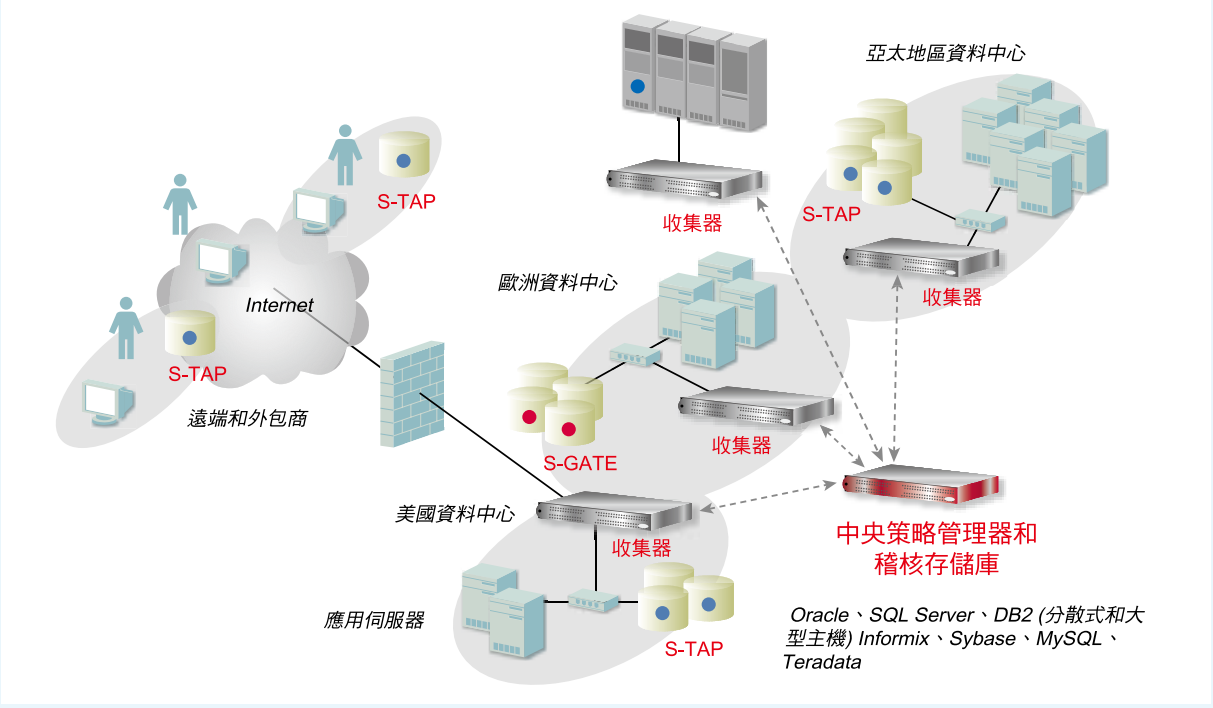
業界最佳報告

Guardium 解決方案包含超過 150 條預先配置的策略和報告，納入我們與全球 1000 家公司、全球四大公司稽核人員和評估人員合作的最佳實務和豐富經驗，幫助解決 SOX、PCI DSS 和資料隱私法等法規需求，簡化資料管理和資料隱私計畫。

除了預先內建的報告範本，Guardium 還提供圖形化拖放介面，助您輕鬆構建新報告或修改現有報告。報告可以自動透過電子郵件，以 PDF 格式（作為附件）或 HTML 網頁連結的形式，發送給使用者，或透過 Web 主控台介面線上查看，也可採標準格式匯至 SIEM 和其他系統。

針對您的企業進行擴展

- 非侵入性：讓資料庫交易 100% 透明，包括專用權使用者的本地存取，且不會影響性能或更改資料庫。
- 獨立於 DBMS：跨平臺解決方案，不依賴本機日誌記錄與稽核。
- 成套的設備：模組化軟體套件構建在加強安全性的 Linux 核心，支援透過「黑盒」設備（完備的儲存、預先安裝的應用、內建管理）進行快速部署。
- 靈活的監控：透過主機的精簡型探測器、SPAN 埠、網路 TAP 或任何組合形式來監控。
- 適合基礎設施：支援 SNMP、SMTP、Syslog、LDAP、Kerberos、RSA SecurID®、變更事件通報管理系統（例如BMC Remedy、CEF），並與所有主流 SIEM 平台整合。
- 多層次：由 Guardium 獨創，可自動將稽核資訊（來自多個系統和位置）聚集和規範於一個集中的稽核儲存庫中。
- 集中管理：透過 Web 主控台對安全策略實施企業級管理。
- 可擴展性：監控的伺服器與流量不斷增加時，可輕鬆增加設備來處理增加的工作量。榮獲專利的智慧儲存演算法所提供的儲存性能，較一般檔案的傳統方法高出 100 倍。
- 防竄改稽核儲存庫：無 root 權限存取和已加密的歸檔的嚴格驗證。
- 基於角色：根據組織角色來控制模組和資料存取。



可擴展的多層次架構：

Guardium 的可擴展性架構同時支援大型與小型環境，集中規範稽核資料，並透過 Web 主控台，對安全策略進行全企業的集中管理。S-TAP 是精簡的主機型探針，可監控所有資料庫流量，包括專用權使用者的本地存取，並將監測資料轉送至 Guardium 收集器設備，進行分析和報告。收集器設備從 S-TAP 及/或直接連接到網路交換機中的 SPAN 埠，收集監控資料。聚合器自動從多個收集器設備，整合稽核資料。為了實現最高的可擴展性和靈活性，您可以配置多層聚合器。擴展 Guardium S-TAP。S-GATE 加強了安全性，並實施了「職權分立」，能夠阻止 DBA 建立新資料庫帳戶與提升現有帳戶專用權。

遵循性工作流程自動化

Guardium獨創的遵循性工作流程自動化應用，能夠簡化整個遵循性工作流程，幫助產生自動化稽核報告、分發給關鍵人員、電子簽署和報告升級。

針對異質環境的統一解決方案

全面的 DBMS 平臺支援

Guardium 的跨平台解決方案，支援所有主流作業系統 (Windows、UNIX、Linux、z/OS) 的主要 DBMS 平台和協定：

支援平臺	支援版本
Oracle	8i, 9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UDB (Windows, Linux, Unix, z/Linux)	8.1, 8.2, 9.1, 9.5
IBM DB2 for z/OS	8.1, 9.1
IBM DB2 UDB for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10, 11
Sun MySQL	4.1, 5, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02

主機監控

S-TAP 是獨創的精簡型軟體探測器，用於在資料庫伺服器的作業系統級別監控網路和本地資料庫協定（共用記憶體、具名管道等）。S-TAP 將所有流量轉給獨立的 Guardium 設備，進行即時分析和報告，而不是依靠資料庫本身來處理和儲存日誌資料，因而對伺服器性能的影響達到最小。S-TAP 一般是首選的探測器，可減少對遠端專用硬體設備與資料中心可用 SPAN 埠的需求。

OS類型	版本	32位元和64位元
AIX	5.1, 5.2, 5.3, 6.1	皆支援
HP-UX	11.00, 11.11, 11.31	皆支援
	11.23 PA	32位元
	11.23 IA64	64位元
Red Hat Enterprise	2, 3, 4, 5	皆支援
SUSE Linux	9, 10	皆支援
Solaris - SPARC	6, 8, 9, 10	皆支援
Solaris - Intel/AMD	10	皆支援
Tru64	5.1A, 5.1B	64位元
Windows	NT	32位元
	2000, 2003, 2008	皆支援

應用監控

Guardium追蹤透過多層次企業應用來存取關鍵表單終端使用者的活動，從而找出潛在詐欺行為，而不是直接存取資料庫，因為企業應用通常使用一種稱為「連接池」(Connection Pooling)的最佳化機制，所有使用者流量都被集中到少量的資料庫連線中，僅能透過通用應用的帳戶名來識別，隱藏了終端使用者的身份。Guardium 支援所有的現成企業主流應用監控。其他的應用（包括內部應用）的支援，則透過在應用伺服器級別監控來實現。

支援的企業應用	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
支援的應用伺服器平台	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform

關於 IBM 子公司 Guardium

Guardium 是 IBM 子公司，致力於透過持續監控對高價值資料庫的存取和變更來保護關鍵企業資訊。Guardium 的可擴展平台可透過異質基礎設施的統一策略，簡化資訊治理，並透過自動化法規遵循流程來降低操作成本，協助企業以安全的方式使用可靠資訊，推動更智慧的業務成果。

目前全球超過 450 個資料中心都採用 Guardium 的企業平台，包括 5 家全球銀行龍頭、前6大保險公司中的 4 家、3 家頂級零售商中的 2 家、20 家全球頂尖電信公司、2 家全球頂級飲料品牌、全球最著名的 PC 廠商、全球 3 大汽車製造商中之一、一家全球前 3 大航空公司，以及一家商業智慧軟體供應龍頭。Guardium 是第一家透過可擴充企業平台解決核心資料安全問題的公司，既能即時保護資料庫，又能自動化完整的法規遵循稽核流程。

台灣國際商業機器股份有限公司
台北市松仁路7號3樓
市場行銷處：0800-016-888按1
技術諮詢熱線：0800-000-700

2010年5月