# IBM InfoSphere Guardium

*管理整個資料庫安全和法規遵循生命週期*

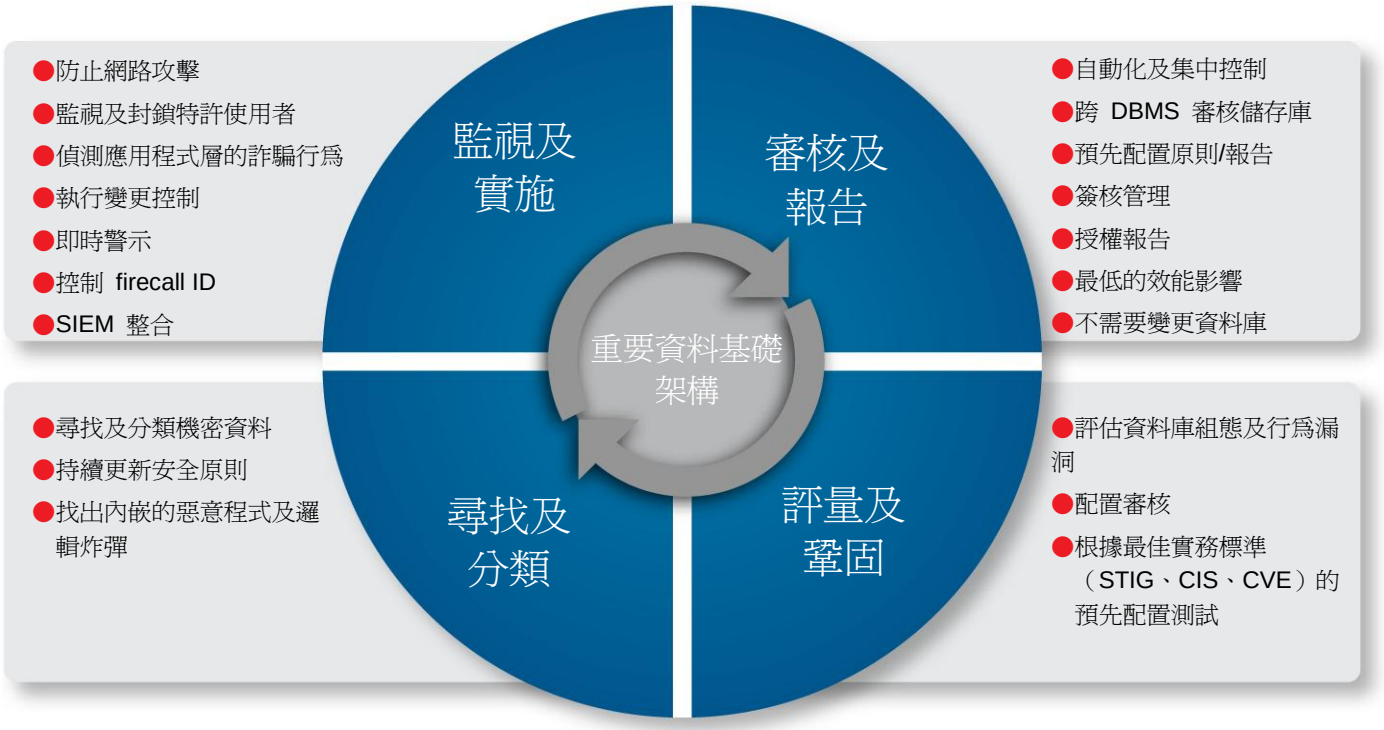
越來越多全球 1000 大機構相信，IBM 比其他技術供應商更能保護重要企業資料。我們提供最簡單強大的解決方案，保護財務和 ERP 資訊、客戶和智慧卡持有者資料以及儲存於企業系統的智慧財產。

我們的企業安全平台可防止特許使用者與潛在駭客的未獲授權或可疑活動，還會監視 Oracle E-Business Suite、PeopleSoft、SAP 這類企業應用程式與內部系統終端使用者可能的詐騙行爲。

同時，我們解決方案的可擴展式多層次架構，可將整個應用程式與資料庫基礎架構的法規遵循控制自動化與集中，盡可能提高作業效率。

然而，這個解決方案傑出的地方不僅僅在於它所能做的事情, 更在於它”沒有”做的事情，比如：幾乎不影響效能、無需調整資料庫，也不需要仰賴原生資料庫日誌或稽核公用程式。

## 即時資料庫安全與監視




*統一的解決方案：*InfoSphere Guardium 以單一統一主控台和後端資料儲存庫爲基礎，提供一系列整合模組，以管理整個資料庫安全及法規遵循生命週期。

InfoSphere Guardium 是獨一無二的解決方案，以統一的 Web 主控台、後端資料儲存庫與工作流程自動化系統，因應整個資料庫的安全與法規遵循生命週期，能讓您：

- 在企業資料庫尋找及分類機密資訊。
- 評量資料庫漏洞與配置缺陷。
- 確保在執行建議的變更後鎖定配置。
- 以支援職權分立的安全防竄改審核追蹤，針對跨平台和通訊協定的所有資料庫交易提供 100% 的可見度和精度。
- 追蹤 Microsoft SharePoint 等各大檔案共享平台上的活動。
- 針對機密資料存取、特許使用者動作、變更控制、應用程式使用者活動與登入失敗這類安全異常監視與執行原則。
- 利用 SOX、PCI DSS 與資料隱私權的預先配置報告，自動化整個法規遵循審核程序，包括將報告配送給監督團隊、簽核與呈報。
- 爲企業層面的法規遵循報告、效能最佳化、調查與鑑識，建立單一的集中審核儲存庫。
- 輕鬆調整，從保護單一資料庫，擴大爲保護全球各地資料中心的眾多資料庫。

## 尋找及分類

**自動尋找、分類與保護機密資訊**

機構建立及維護的數位資訊量越來越多，尋找及分類機密資訊也日益困難。

針對經歷過合併或收購的機構，或者舊系統原始開發人員已經離開的環境，尋找及分類機密資訊尤其困難。即使在最理想的狀態下，爲支援新商業需求而持續變更應用程式與資料庫結構，還是會輕易使靜態安全原則失效，導致機密資料狀態不明並失去保護。

機構的難題如下：

- 規畫所有含機密資訊的資料庫伺服器，並且瞭解從所有來源（業務單位應用程式、批次程序、特定查詢、應用程式開發人員、管理員）存取機密資訊的方式。
- 在儲存資訊機密狀態不明時，保護資訊及管理風險。
- 在不確定哪些資訊受特定法規條款約束時，確保法規遵循。

若使用 InfoSphere Guardium，您可使用資料庫自動探索與資訊分類找出機密資料儲存位置，然後使用自訂的分類標籤，自動強制執行安全原則，套用至特定機密物件類別。這些原則會確保僅限授權使用者檢視及/或變更機密資訊。

您還可以排程定期探索機密資料，以免欺詐伺服器入侵，並確保不會「遺忘」重要資訊。

## 評量及鞏固

**漏洞、配置與行爲評量**

InfoSphere Guardium 的資料庫安全評量會掃描整個資料庫基礎架構，查看是否有漏洞，並使用即時和歷程資料，提供資料庫安全狀況的後續評估。

InfoSphere Guardium 的資料庫安全評量根據業界最佳實務（CVE、CIS、STIG）提供全面的預先配置測試庫及平台特有漏洞，並透過 InfoSphere Guardium 的 Knowledge Base 服務定期更新。您還可搭配特定需求定義自訂測試。評量模組也會盡力找出法規遵循相關漏洞，例如未獲授權存取保留的 Oracle EBS 與 SAP 表格，以遵循 SOX 與 PCI DSS。

評量分爲兩大類：

- 漏洞與漏洞配置測試檢查，例如遺漏的修補程式、配置不當的專用權和預設帳戶。
- 行爲測試會即時監視所有資料庫資料流量，根據存取與操作資料庫的方式找出漏洞，例如失敗登入次數過多、用戶端執行管理指令，或在非工作時間登入。

除了使用往下探查功能產生詳細報告，評量模組還會以加權指標（根據最佳實務）、業界標準參照號碼來產生安全性能報告卡，並建議加強資料庫安全的具體行動計畫。

**配置鎖定與變更追蹤**

執行漏洞評量產生的建議動作後，便可建立安全配置基準線。若使用 InfoSphere Guardium 的 Configuration Audit System (CAS)，則可監視此基準線的任何變更，並且確定變更不是由未授權變更控制原則和程序所執行。

## 監視及實施

**監視與執行資料庫安全和變更控制原則**

InfoSphere Guardium 提供精細的即時原則，避免特許資料庫帳戶未獲授權或可疑的動作，以及來自欺詐使用者或外來者的攻擊。您也可以利用透過 Oracle EBS、PeopleSoft、Siebel、SAP、Cognos 這類常見服務帳戶，以及採用 IBM WebSphere、Oracle WebLogic 和 Oracle AS 這類應用程式伺服器自訂系統存取資料庫的多層應用程式，找出未獲授權變更資料庫的應用程式使用者。

此解決方案可由資訊安全人員管理，無需資料庫管理員 (DBA) 介入。您也可定義精細的存取原則，根據 OS 登入、IP 或 MAC 位址、來源應用程式、時段、網路通訊協定與 SQL 指令類型，限制特定表格的存取。

**所有資料庫資料流量的連續環境定義分析**

InfoSphere Guardium 會使用正在申請專利的語言分析，根據每筆 SQL 交易的「執行人、執行內容、執行地點、執行時間與執行方式」這類詳細環境定義資訊偵測未獲授權的動作，即時連續監視所有資料庫作業。這種獨特的方式有別於僅尋找預先定義模式或簽章的傳統方式，可減少誤判情形，而且控制能力無與倫比。

**基準化偵測異常行爲並自動化原則定義**

系統會建立基準線並同時識別正常商業程序與疑似異常的活動，自動建議您可用來預防 SQL 資料隱碼這類攻擊的原則。您可從直覺式下拉功能表輕鬆新增自訂原則。

**主動的即時安全**

InfoSphere Guardium 提供豐富主動回應未獲授權或異常行爲的即時控管。原則型動作可包含即時安全警示（SMTP、SNMP、

Syslog）；軟體封鎖；啓用完整記載；隔離使用者；以及 VPN 連接埠關閉及與周邊 IDS/IPS 系統協調這類自訂動作。

**追蹤與解決安全事件**

法規遵循法規規定，機構必須記錄、分析、即時解決所有事件，並向管理階層報告。InfoSphere Guardium 提供商業使用者介面、解決安全事件的工作流程自動化，以及用以追蹤開放事件數、嚴重性層次與事件開放持續時間這類重要指標的儀表板。

## 審核及報告

**掌握精細的審核追蹤**

InfoSphere Guardium 以連續且精細的方式審核追蹤所有資料庫活動，並且即時以環境定義的方式分析與過濾，以執行主動控制並產生審核者所需的特定資訊。

得出的報告會詳細顯示所有的資料庫活動，例如登入失敗、提高專用權、變更綱目、在非工作時間或從未獲授權應用程式存取，以及存取機密表格，以證明法規遵循狀況。例如，系統會監視下列所有情況：

- 安全異常，例如 SQL 錯誤與登入失敗。
- 變更資料庫結構的 Create/Drop/Alter Tables 這類 DDL 指令，對於 SOX 等資料控管規定尤其重要。
- SELECT 查詢，這些對於 PCI DSS 等資料隱私權規定尤其重要。
- DML 指令（Insert、Update、Delete），包括綁定變數。
- 控制帳戶、角色與權限（GRANT、REVOKE）的 DCL 指令。
- 每個 DBMS 平台，例如 PL/SQL (Oracle) 與 SQL/PL (IBM) 支援的程序化語言。
- 資料庫執行的 XML。
- SharePoint 物件的變更。

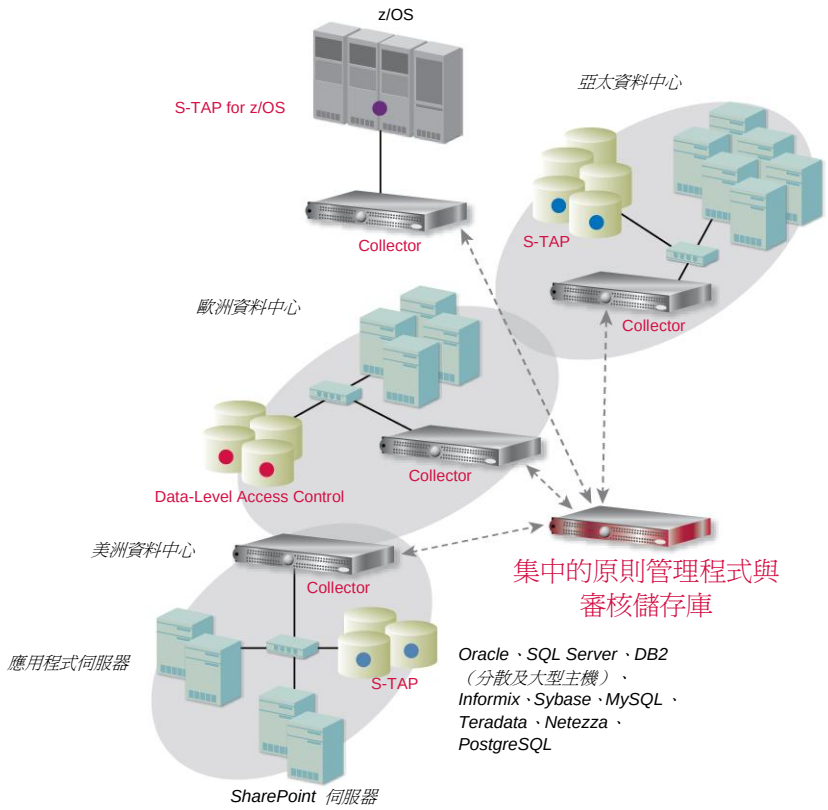
**最佳報告**

InfoSphere Guardium 解決方案包含 150 多個預先配置原則與報告，參考最佳實務以及與全球 1000 大企業、Big 4 審核者和全球評量員合作的經驗。這些報告有助於因應法規需求，例如 SOX、PCI DSS 與資料隱私權法，並且能精簡資料控管和資料隱私權方案。

除預先內建的報告範本，InfoSphere Guardium 還提供圖形式拖放介面，可輕鬆建立新報告或修改現有的報告。報告可自動用 PDF 格式（當成附件）或 HTML 頁面連結，以電子郵件寄給使用者。報告也可透過 Web 主控台介面線上檢視，或以標準格式匯出至 SIEM 和其他系統。

## 可配合企業調整

- **非侵入性：**完全掌握所有資料庫交易，包括特許使用者的本端存取，對效能影響微乎其微，而且無需變更資料庫或應用程式。
- **不受限於 DBMS：**跨平台解決方案，不仰賴原生記載或審核。
- **以裝置爲基礎：**模組化軟體套組，建置於強大的 Linux Kernel，透過「黑盒」裝置（獨立儲存體、預先安裝的應用程式、內建的管理）加速部署。另以虛擬裝置方式提供，可支援硬體合併策略。
- **彈性監視：**透過輕量主機型探測器、SPAN 連接埠、網路 TAP 或任何組合。
- **備妥的基礎架構：**支援 SNMP、SMTP、Syslog、LDAP、Kerberos、RSA SecurID®、變更票務系統，例如 BMC Remedy、CEF 以及整合各大 SIEM 平台。
- **多層：**InfoSphere Guardium 業界獨一無二的功能，將來自多個資料庫平台和位置的審核資訊，自動彙整與正規化至單一集中的審核儲存庫。
- **集中管理：**透過 Web 主控台管理企業層面的跨 DBMS 安全原則。
- **可擴展性：**監視的伺服器或資料流量越來越多時，只要新增裝置便能處理增加的負載。專利的智慧型儲存演算法，遠勝於傳統 FAT 檔案型方式的儲存效率。
- **防竄改審核儲存庫：**強型態鑑別沒有根存取和加密保存。
- **以角色爲基礎：**根據機構角色控制模組與資料的存取。




***可調式多層架構：***

InfoSphere Guardium 的可調式架構同時支援大型和小型環境，集中彙整與正規化審核資料，並透過 Web 主控台集中管理企業層面的安全原則。 S-TAP 屬於輕量型主機式探測器，可監視所有資料庫資料流量，包括特許使用者的本端存取，然後轉送給 InfoSphere Guardium 收集器裝置進行分析與產生報告。 收集器裝置會收集 S-TAP 的監視資料，及/或直接連線至網路交換器的 SPAN 連接埠。 彙整工具會自動彙整來自多個收集器裝置的審核資料。 您可配置多層彙整工具，提高可調整性和彈性。 另外，InfoSphere Guardium 的 Data-Level Access Control 是以 S-TAP 延伸的方式執行，會封鎖 DBA，不允許執行安全功能，例如建立新資料庫帳戶及提高現有帳戶的專用權，以加強安全及執行職權分立。

### 法規遵循工作流程自動化

InfoSphere Guardium 的 Compliance Workflow Automation 是業界獨一無二的應用程式，協助將審核報告產生、發送給主要利害關係人、電子簽核與呈報的程序自動化，簡化整個法規遵循工作流程程序。使用者完全可以詳細自訂工作流程程序，讓特定審核項目一直到簽核前都可個別遞送及追蹤。

## 異質環境的統一解決方案

### 支援多種平台

InfoSphere Guardium 的跨平台解決方案支援各大 DBMS 平台和執行於各大作業系統（Windows、UNIX、Linux、z/OS）的通訊協定，以及 Microsoft SharePoint 和 FTP 環境：

| 支援的平台 | 支援的版本 |
|---|---|
| Oracle Database | 8i、9i、10g（r1、r2）、11g、11gR2 |
| Oracle Database（ASO、SSL） | 9i、10g（M、r2）、11g |
| Microsoft SQL Server | 2000, 2003, 2008 |
| Microsoft SharePoint | 2007, 2010 |
| IBM DB2（Linux、Unix、Linux for System z） | 9.1, 9.5, 9.7 |
| IBM DB2 (Windows) | 9.1, 9.2, 9.5, 9.7 |
| IBM DB2 for z/OS | 7, 8, 9 |
| IBM DB2 for iSeries | V5R2、V5R3、V5R4、V6R1 |
| IBM Informix | 7, 9, 10, 11,11.50 |
| Sun MySQL 與 MySQL Cluster | 4.1, 5.0, 5.1 |
| Sybase ASE | 12, 15, 15.5 |
| Sybase IQ | 12.6, 15 |
| Netezza | 4.5 |
| PostgreSQL | 8 |
| Teradata | 6.X、12、13 |
| FTP | |

### 主機型監視

S-TAP 屬於輕量型軟體探測器，堪稱業界獨一無二，可在資料庫伺服器的 OS 層次，同時監視網路和本端資料庫通訊協定（共用記憶體、具名管道等）。S-TAP 會將所有資料流量轉送給個別 InfoSphere Guardium 裝置進行即時分析與產生報告，而非仰賴資料庫本身處理及儲存日誌資料，減少對伺服器效能的影響。S-TAP 備受青睞，因爲無需在遠端位置或資料中心的可用 SPAN 連接埠有專用的硬體裝置。

| OS 類型 | 版本 | 32 位元與 64 位元 |
|---|---|---|
| AIX | 5.1, 5.2, 5.3, | 兩者皆有 |
| | 6.1 | 64 位元 |
| HP-UX | 11.00, 11.11, 11.23, 11.31 | 兩者皆有 |
| Red Hat Enterprise Linux | 3, 4, 5 | 兩者皆有 |
| Red Hat Enterprise Linux for System z | 5.4 | |
| SUSE Enterprise Linux | 9, 10, 11 | 兩者皆有 |
| SUSE Enterprise Linux for System z | 9, 10, 11 | |
| Solaris - SPARC | 8, 9, 10 | 兩者皆有 |
| Solaris - Intel/AMD | 10 | 兩者皆有 |
| Tru64 | 5.1A、5.1B | 64 位元 |
| Windows | 2000, 2003, 2008 | 兩者皆有 |
| iSeries | i5/OS* | |

** 支援網路活動監視、透過 Enterprise Integrator 支援本端活動*

**應用程式監視**

InfoSphere Guardium 會追蹤透過多層企業應用程式，而非直接存取資料庫來存取重要表格的終端使用者活動，找出可能的詐騙行爲。這屬於必備功能，因爲企業應用程式通常使用所謂的「連接池」最佳化機制。在儲存區環境中，所有使用者資料流量都會彙整於幾個資料庫連線，唯一的辨識方式是通用應用程式帳戶名稱，因此隱藏了終端使用者的身分。InfoSphere Guardium 支援各大市售企業應用程式的應用程式監視。以在應用程式伺服器層次監視交易的方式，支援其他應用程式，包括內部應用程式。

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

## 關於 IBM InfoSphere Guardium

Guardium 是 IBM InfoSphere 整合平台的一部分，此整合平台可定義、整合、保護及管理系統的可靠資訊。InfoSphere Platform 可根據共用中介資料與模式的核心整合，提供可靠資訊的所有基礎建置區塊，包括資料整合、資料倉儲、主要資料管理，以及資訊控管。此模組化產品可讓您隨時啓用，並將 InfoSphere 軟體建置區塊與其他供應商的元件混合搭配使用，或選擇同時部署多個建置區塊，以提高速度和價值。InfoSphere Platform 可爲資訊密集的專案提供企業級基礎，以簡化難題並爲企業快速提供可靠資訊，進而達到最佳效能、可調整性、可靠性及加速功能。



110 台北市松仁路 7 號 3 樓
技術諮詢熱線：0800-000-700
台北市松仁路 7 號 3 樓



台灣印製

2010 年 5 月



請回收

**InfoSphere®**
**軟體**