IBM InfoSphere Guardium

管理企業系統整個資料安全性和法規遵循生命週期

全球頂尖組織都仰賴 IBM，為其重要的企業資料提供保護。 但實際上我們提供的是簡易強大的解決方案，能夠保護財務和 ERP 資訊、客戶和持卡人資料及智慧財產等結構化與非結構化資料，適用於各種企業系統，包括資料庫、資料倉儲、檔案共用，以及像是雲端、虛擬和 Hadoop 系統等新型資料中心環境。

我們的企業安全平台可防止特許內部人員與潛在駭客的未獲授權或可疑活動，還可監控 Oracle E-Business Suite、PeopleSoft、SAP 這類企業應用程式與內部系統使用者可能的詐騙行為。

同時，我們的解決方案採用可調式多層架構，可將整個資料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，除了此解決方案賦與之功能外，更不幾乎不影響其他相關之效能、無需調整資料來源，也不需要仰賴原生日誌或審核公用程式。

此外，IBM 瞭解資料防護不只是一項獨立的工作，而是必須整合到企業資訊控管和資訊技術 (IT) 安全性策略之中。我們的資料防護於供應時便能立即與這兩種計劃協同整合，快速獲得投資報酬。

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為基礎，提供一系列整合模組，以管理整個資料安全及法規遵循生命週期。

IBM® InfoSphere® Guardium® 提供一系列整合模組，以管理整個資料安全及法規遵循生命週期。

InfoSphere Guardium 解決方案提供統一網頁主控台、後端資料儲存庫和工作流程自動化系統，能夠應對即時資料安全性及法規遵循生命週期的所有領域，讓您：

- 持續監控對資料庫、資料倉儲、Hadoop 系統和檔案共用等異質資料儲存庫的存取，即時保護機密資料 (結構化及非結構化)。
- 透過支援職權分立的安全防竄改稽核追蹤，來擷取並檢驗資料流量，包括特許使用者經由支援的平台及通訊協定的本機存取。
- 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性例外事項，監控與施行原則。
- 尋找並分類異質資料基礎架構中的機密資料，同時識別其目前的授權。
- 評估資料基礎架構中的漏洞及組態風險。確保在執行建議的變更後鎖定組態。
- 為企業層面的法規遵循報告、效能最佳化、調查與鑑識，建立單一的集中稽核儲存庫。將整個資料法規遵循稽核流程自動化，包括將報告散佈給監控團隊、簽核及呈報，還有預先設定的 SOX、PCI 資料安全標準 (DSS) 和資料隱私權報告。
- 可從保護單一資料來源，輕鬆擴充為保護全球各地資料中心的數千個資料來源。
- 這種統一的方法可廣泛支援客戶的關鍵資料環境：
- 結構化和非結構化資料 (資料庫、資料倉儲、檔案共用、大型資料環境)
- 分散式及主機環境
- 虛擬化、雲端及傳統基礎架構
- 套裝及自訂應用程式 (交易及大範圍應用程式，如 CRM)

尋找及分類

組織所建立及維護的數位資訊量越來越龐大，因此要找出所有相關的機密資訊也變得極為困難，更別說要進行分類，而且還要判斷資料存取權的擁有者 (以及應該擁有的使用者)。

尋找並分類機密資訊

對經歷過併購或現有系統使用年限比原始開發人員還久的組織來說，尋找並分類機密資訊尤其困難。即使在最好的情況下，為了支援新商業需求所需的應用程式及資料來源 (如資料庫結構) 的持續性變更，會輕易讓靜態的安全性原則失效，使得機密資料變得分散且不受保護。

組織的難題如下：

- 對應包含機密資訊的所有資料來源，判斷哪些人擁有存取權，並瞭解所有來源的存取方式 (業務單位應用程式、批次流程、特定查詢、應用程式開發人員、管理員等)。
- 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。

自動探索、分類及保護機密資訊

若使用 InfoSphere Guardium，您可使用資料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，自動施行套用至特定機密物件類別的安全原則。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。

監控及稽核

對機密資料的安全威脅不斷攀升，再加上法規遵循命令持續擴充，促使組織必須尋求有效的方式來監控整個企業的資料活動，並即時遏止未授權的活動。

對資料來源的所有流量進行持續監控和環境定義分析

InfoSphere Guardium 即時監控企業資料來源，包括資料庫、資料倉儲、檔案共用和 Hadoop 型系統等來源，進而施行原則並保護機密資料。

InfoSphere Guardium 使用語言分析，按照每個資料存取的「對象、內容、位置、時間和方式」等詳盡的環境定義資訊，偵測未授權的動作，以持續即時監控所有資料存取作業。這種環境定義方式可減少誤判，同時提供足夠的控制層級，而不是像傳統的方法，只會從資料庫流量或稽核日誌中查看預先定義的模式或跡象。

此外，您還可偵測間接攻擊，例如欺詐使用者偽裝成應用程式伺服器的使用者，或是繞過多層應用程式所使用的存取控制設定時。這些情況都會發生在 Oracle E-Business Suite、PeopleSoft、Siebel、SAP、IBM Cognos® 軟體等應用程式環境，以及內建於 Oracle WebLogic、Oracle AS 等應用程式伺服器和 IBM WebSphere® 系列產品內的自訂系統。

掌握精細的稽核追蹤

數量不斷成長的資料通常散佈在整個企業內，使得組織越來越難擷取及分析檢驗法規遵循所需的詳盡稽核追蹤。

InfoSphere Guardium 以連續且精細的方式追蹤所有資料存取活動，並且即時以環境定義的方式分析與過濾，以執行控制並產生稽核者所需的特定資訊。

可從產生的報告中檢視詳細的資料存取活動，例如登入失敗、權限升級、配置變更、關機期間存取，或來自未授權應用程式及機密表格存取，以展示法規遵循情形。例如，系統可監控資料庫中的下列情況：

- 安全性例外事項，例如 SQL 錯誤
- 變更結構的 CREATE/DROP/ALTER 這類指令，對於 SOX 等資料控管規定尤其重要
- SELECT/READ/OPEN 指令，對於 PCI DSS 等資料隱私權規定尤其重要
- 資料操作指令 (例如 INSERT、UPDATE、DELETE)，包含綁定變數

- 控制帳戶、角色及權限的資料控制語言指令 (GRANT、REVOKE)
- 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
- Microsoft SharePoint 物件的變更

追蹤與解決安全事件

法規遵循法規規定，組織必須記錄、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、嚴重程度與事件開放持續時間等重要指標的儀表板。

最佳報告

InfoSphere Guardium 解決方案包含 150 多個預先配置的原則與報告，參考最佳實務以及與全球 1000 大企業、主要稽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（當成電子郵件附件）或 HTML 頁面連結寄給使用者。報告也可透過 Web 主控台線上檢視，或以標準格式匯出至 SIEM 及其他系統。

法規遵循工作流程自動化

InfoSphere Guardium 法規遵循工作流程自動化應用程式可簡化整個法規遵循工作流程，有助於自動產生稽核報告、發送給主要利害關係人、執行電子簽核與呈報。工作流程可完全由使用者自訂；特定的稽核項目可透過簽核個別引導及追蹤。

施行及保護

施行即時資料安全性及變更控制原則

InfoSphere Guardium 提供精細的即時原則，避免特許使用者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。

不需要驚動資料庫管理員 (DBA) 等資料操作員，資訊安全人員即可管理解決方案。您也可定義精細的存取原則，根據作業系統登入、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，限制特定表格或物件的存取。

主動的即時安全

InfoSphere Guardium 提供即時控制，在未獲授權或異常行為造成嚴重傷害之前作出回應。原則型動作可包含即時安全警示 (SMTP、SNMP、Syslog)；軟體封鎖；完整記載；使用者隔離；以及自訂動作，像是關閉 VPN 連接埠及協調周邊的 IDS/IPS 系統。此外，InfoSphere Guardium 還會將警示和稽核報告傳送給 IBM Security QRadar 和其他的 SIEM 解決方案，以深入的資料活動發現為基礎，進行資訊更充足的跨 IT 安全智慧分析。

基準化偵測異常行為並自動化原則定義

系統會建立基準線並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。直覺化選單，方便新增自訂原則。

評估及鞏固

資料基礎架構為高動態性，且經常會變更帳戶、組態及修補程式。多數組織缺乏集中控制或技能熟練的資源，無法檢閱系統的變更，判斷是否出現安全弱點。

自動評估漏洞、組態與行為

InfoSphere Guardium 的資料安全性評估功能可掃描整個資料基礎架構中的漏洞，運用即時和歷史資料持續評估資料安全性態勢。

以業界最佳實務 (CVE、CIS、STIG) 為基礎，提供完善預先設定的測試資料庫，再加上平台特定漏洞，可透過 InfoSphere Guardium Knowledge Base 服務定期更新。您還可搭配特定需求定義自訂測試。評估模組可標記出法規遵循相關漏洞，例如未獲授權存取保留的 Oracle E-Business Suite 與 SAP 表格，以遵循 SOX 與 PCI DSS。

評估分為兩大類：

- **漏洞與組態測試檢查**：例如遺漏的修補程式、不當組態的專用權和預設帳戶。
- **行為測試**：即時監控所有資料流量，按照資料來源的存取及管理以找出弱點，例如大量登入失敗、執行管理指令的用戶端，或下班時間的登入。

除了產生詳細報告及支援的資料，評估模組還會產生安全性健康報告卡。報告卡不只包含以最佳實務為基礎的加權指標和產業標準參考編號，也會建議行動計劃以強化資料安全性。還可針對這些動作進行設定，以遵循支援 FISMA 法規的 Security Content Automation Protocols(SCAP) 格式等報告標準。

組態鎖定與變更追蹤

執行漏洞評估中所建議的動作後，您也可以建立安全的組態基準線。InfoSphere Guardium 組態稽核系統可監控基準線的變更，確定未超出授權的變更控制原則及程序。

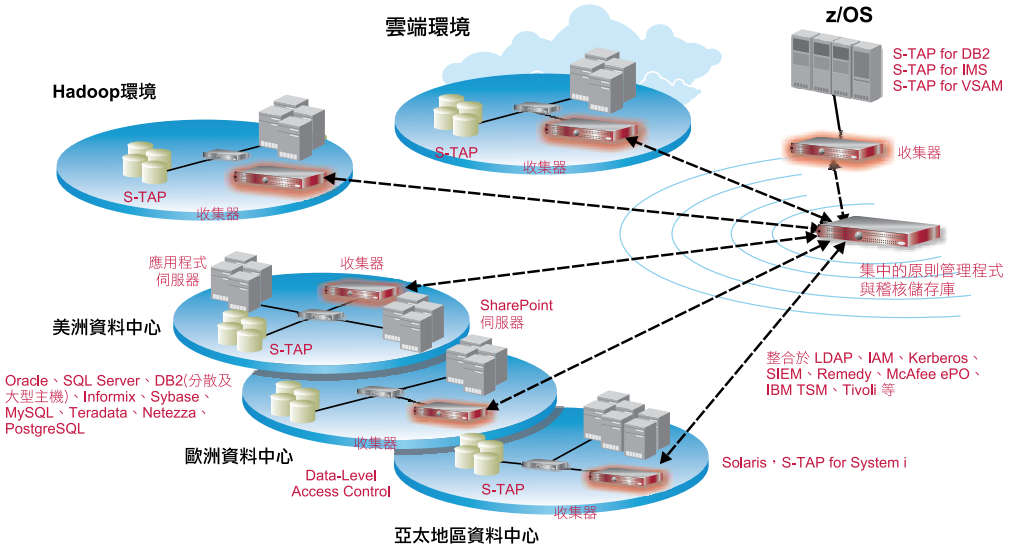
異質環境的統一解決方案

多數組織都有來自多家廠商，部署不同作業系統的多個資料庫，因此難以施行統一的安全原則，並從整個企業內收集一致的稽核資訊。由於異質環境的存在，導致必須依不同平台採用各自獨立方式來儲存安全和法規遵循活動，因而提高作業成本，消耗寶貴資源。

成本最低的全企業層面擴充能力

InfoSphere Guardium 可使用內建的自動化及整合功能，降低作業成本，隨著稽核需求及環境作出調整，輕鬆擴充。無論系統具備何種規模，InfoSphere Guardium 都能簡化作業，提供：

- **單一解決方案**。完善的平台支援和廣泛的功能，包括主動防護等，可將單一解決方案部署到整個企業。
- 非侵入式設計。不需變動現有的資料庫、應用程式或網路組態，也不需仰賴原生日誌，就能將對效能的影響降到最低。
- **投資保障**。監控伺服器的數量不斷增加，但只要使用「網格」增加容量，就能保存原則及法規遵循工作流程等現有的 InfoSphere Guardium 採購和組態投資。
- **簡化管理**。使用 Central Policy Manager 內的單一介面來管理應用裝置和探測器，包括組態、使用者管理和軟體更新。探測器更新後不需重新啟動。STAP 已包含在 IBM DB2 10 等平台內。
- **全企業層面的分析及報告功能**。透過 Central Policy Manager 進階的報告及分析功能，自動將來自多重資料來源和收集器的稽核資訊標準化，並彙整到單一、安全、集中化的稽核儲存庫。
- **工作自動化**。系統具備減少手動工作的能力，例如整合式法規遵循工作流程自動化、廣泛的指令集自動化 API 支援、組態稽核範本、自動在功能間共用資訊等。
- **部署彈性**。以軟硬體形式，透過預先設定的應用裝置供應，支援各種成本縮減策略。支援使用輕量化的主機型探測器，透過網路或各種組合方式來監控，將能見度提升至最高。
- **基礎架構整合**。自動與系統整合，包含 LDAP、管理資料庫、電子郵件、變更票證和 Syslog，以及 SIEM 解決方案 (例如 IBM Security QRadar)，省去手動交換安全資訊。
- **負載平衡及容錯轉移**。組態具備彈性，可隨網路變更和故障進行調整，將高成本的故障問題降到最低。



可擴充的多層架構，支援大型和小型環境，可集中彙整及標準化稽核資料，集中管理全企業層面的安全原則。S-TAP 屬於輕量型主機式探測器，可監視所有資料流量，包括特許使用者的本機存取，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 的監控資料，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稽核資料。可設定多層的彙整工具，以增加彈性及擴充能力。InfoSphere Guardium Data-Level Access Control 可執行為 S-TAP 的延伸套件，強化安全性並施行職權分立，像是阻止 DBA 建立新的資料庫帳戶、提升現有帳戶的權限等。

支援多種平台

Guardium 支援各種主要的 DBMS 平台和在主要作業系統上執行的通訊協定，並支援各種不斷成長的檔案和文件共用環境。

支援的平台	支援的版本
Cloudera	CDH3 Update 2、3、4
CDH4	
Oracle Database	9i、10g(r1、r2)、10g、11gR1、11gR2、11g RAC
Microsoft SQL Server	MS SQL Cluster、2000、2005、2005 x64、2005 IA64、2008、2008 x64、2008 IA64、2008 R2 x64/x32/ 叢 集、2012
Microsoft Sharepoint	2007、2010
Microsoft Windows 檔案共用	2003、2008
IBM BigInsights	1.4
IBM DB2 for Linux、UNIX 和 Windows	9.1、9.5、9.7、9.8 (DB2 pureScale)、10.1
IBM DB2 for System i	V5R2、V5R3、V5R4、V6R1
IBM DB2 for z/OS	8.1、9.1. 10.1
IBM Informix	10、11、11.50、11.70
IBM Netezza	NPS 4.5、4.6、4.6.8、5.0、6.0、6.02
IBM IMS	9、10、11、12
IBM VSAM	請參閱作業系統支援表中的 z/OS 支援。
Sun MySQL 與 MySQL Cluster	4.1、5.0、5.1、5.5
* 支援網路活動監視、透過 Enterprise Integrator 支援本機活動	
Sybase ASE	15、15.5、15.7
Sybase IQ	15.0、15.1、15.2、15.3、15.4
Teradata	12、13、13.10、14
PostgreSQL	8、9、9.03、9.04
FTP	

主機型監視

S-TAP 屬於輕量型軟體探測器，可在資料庫伺服器的作業系統層次，同時監視網路和本機資料庫通訊協定 (例如共用記憶體、具名管道)。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，因為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。

本表顯示目前 S-TAP 可用的所有作業系統平台和版本

作業系統	版本	32 位元與 64 位元
IBM AIX	5.3	兩者皆有
	6.1、7.1	64 位元
HP-UX	11.11、11.23、11.31	64 位元
Red Hat Enterprise Linux	4、5、6	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	9、10、11	兩者皆有
Solaris – Intel/AMD	10	兩者皆有
	11	64 位元
Windows Server	2003、2008	兩者皆有
IBM i	6.1、7.1	
z/OS	1.11、1.12	

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使用者活動，找出可能的詐騙行為。這屬於必備功能，因為企業應用程式通常使用所謂的「連線儲存區」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，因此隱藏了使用者身分。InfoSphere Guardium 支援各大市售企業應用程式的應用程式監視。另外則透過監控應用程式伺服器層級的交易，或傳送到 InfoSphere Guardium 通用摘要，提供對其他應用程式，包括家用應用程式的支援。IBM 提供通用摘要通訊協定的說明文件，讓組織能夠執行適用其特殊環境的介面，以支援 InfoSphere Guardium 所支援的監控及防護功能中的任何子集。Infosphere Guardium 也會從 WAF 流量擷取摘要，使用其原則進行分析。

支援的企業應用程式	• Oracle E-Business Suite • Oracle PeopleSoft • Oracle Siebel • SAP • SAP BusinessObjects Web Intelligence • IBM Cognos • F5 Web Application Firewall
支援的應用程式伺服器平台	• IBM WebSphere • Oracle WebLogic Server • Oracle Application Server • JBoss Enterprise Application Platform • + 其他以客戶需求為依據的平台

關於 IBM InfoSphere Guardium

InfoSphere Guardium 屬於 IBM InfoSphere Integrated Platform 及 IBM Security Systems Framework 的一部分。InfoSphere Integrated Platform 為您系統內的可靠資訊提供定義、整合、保護及管理服務。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啟用，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 可為資訊密集的專案提供企業級基礎，以簡化難題並為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。

如需進一步瞭解 IBM Guardium，請造訪 ibm.com/guardium

IBM Corporation
軟體事業處
技術諮詢熱線：0800-000-700
台北市松仁路 7 號 3 樓

台灣印製
2012 年 12 月

InfoSphere software

IMD14286-USEN-03