Information Management

IBM

企業資料庫安全與監控

Enterprise Database Security & Monitoring

Data Management

Paul Chang
paulyc@tw.ibm.com

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

新版個資法的實施時程及對企業的主要影響簡介

- 1995/07/12 立法院三讀通過「電腦處理個人資料保護法」
- 1996/05/01 電腦處理個人資料保護法施行細則發佈實施，規定政府與八大行業（徵信、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播）
- 1997 ~ 2010/03 11次修法擴大非公務機關適用產業 (如: 百貨公司業及零售式量販業電腦處理個人資料辦法，無店面零售業 ...)
- 2010/04/27立法院三讀通「個人資料保護法」，適用於所有公務、非公務機關及個人(老闆與經手員工) 。施行日另訂，預測約為2011年六月開始施行 (於施行細則公佈後)
- 新版個資法包含所有個人資料之蒐集、處理及利用， 含紙本資料而非前法案訂定僅針對電腦處理之個人資料，以及如護照號碼、健康檢查資訊...等之前未含括之個資範圍

新版個資法的實施時程及對企業的主要影響簡介(續)

- 鼓勵由財團法人或公益團體協助一般受損害之個人提起團體訴訟
- 民事賠償責任上升：賠償上限由原來之兩千萬變成兩億（且若證明事實損害若大於兩億的話則以事實為限）
- 強調非公務機關須免費提供個資當事人拒絕利用其個人資料進行行銷之機制
- 企業必須自行舉證沒有違反個資法。
- 企業非直接向當事人當事人蒐集的個人資料，必須在法案實施一年內告知當事人。當事人必須書面同意才能使用。
- 故意及非故意都罰：
  - 非故意而產生損害 -> 2年以下有期徒刑、拘役或併科罰金20萬以下
  - 意圖營利 -> 5年以下有期徒刑、拘役或併科罰金100萬以下

個人資料保護法適用情況

- 第一條 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。
- 第二條 本法用詞，定義如下：
  - 一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
  - 二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
  - 三、蒐集：指以任何方式取得個人資料。
  - 四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
  - 五、利用：指將蒐集之個人資料為處理以外之使用。
  - 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。
  - 七、公務機關：指依法行使公權力之中央或地方機關或行政法人。
  - 八、非公務機關：指前款以外之自然人、法人或其他團體。（原僅規範徵信、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播）
  - 九、當事人：指個人資料之本人。

企業需要保護的資料除了個人資料以外，還包括營業秘密

個人資料　　（被動，法律損失或商譽損失）

- 個人資料是指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料；
- 個人資料保護不好，可能造成的是法律賠償與訴訟費用，以及商譽的損失

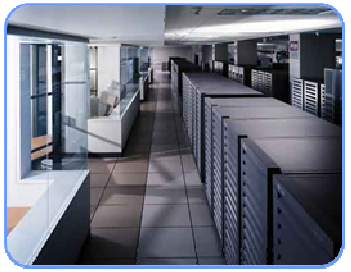
營業秘密　　（主動，直接造成營運損失）

- 營業秘密是指不為公眾所知悉(不公開的)，能為權利人帶來經濟利益，具有實用性並經權利人採取保密措施的技術資訊和經營資訊；
- 營業秘密的洩漏會直接造成企業之營運損失、核心競爭力下降

各行業都的營運秘密資料，如：製程流程與參數、財務資料、員工個人資料、客戶個人資料...。而且從外部入侵或在內部盜取都可能發生

行業別	營運秘密	個人資料
科技及製造業	製程流程與參數、設計資訊、未公開產品規格、軟體原始碼、營運及業務、財務、人事資訊	雇員個人資訊
金融行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	雇員個人資訊、客戶個人資訊、信用卡或帳戶資訊
醫療行業	實驗數據、業務、財務、人事資訊	雇員個人資訊、病患個人資訊、病歷資訊、健康檢查資訊
教育行業	研究報告、業務、財務、人事資訊	教職員資訊、學生及家長個人資訊、學生學習紀錄
政府及軍事	軍事機密資訊、內部調查資料、未公開規劃、稅務資訊、情報資訊	國民、市民資訊、個人稅務及財務資訊、
零售行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	會員資訊、信用卡或帳戶資訊

您的企業是否暴露在以下的風險之下?



內部威脅

未授權的資料變更 e.g. 用戶資料竄改

機密資料洩漏 e.g. 用戶資料外流

外部威脅

駭客、木馬入侵 e.g. 竊取機密產品資訊

法規遵從

資安機制趕不上最新法規要求 e.g. 法律訴訟及行政責罰

國內的個資外洩問題不斷且常成為媒體焦點，將會加速個資法修正進程，跡象顯示內部人員行為和外界的入侵同等重要

出賣考生個資 博暐判賠349萬

*Source: 聯合報

【聯合報／記者呂開瑞 BLOG ／桃園報導】 2009.06.07 02:29 am

台中市博暐公司承包去年國中基測業務，以50萬元販賣考生資料3萬4千多筆給補教業者，主辦基測的國立桃園高中向博暐訴請每洩漏一人罰100元的懲罰性賠償，桃園地院昨天判博暐應賠償349萬餘元。

桃園地院調查，博暐公司標到97年國中基測事務，負責基測的電腦報名、建立各國中集體報名和[redacted]數加密電子檔等，還與主辦的國立桃園高級中學簽定「[redacted]元」的契約。

盜賣資料

桃園法院指出，博暐公司負責人因積欠債務，有意利用考生資料牟利，透過中間人物色買考生個人資料的補習班，隨後以50萬元的價碼，將台中地區、彰化、南投等地的3萬4965名考生的基本資料和測驗分數燒成光碟後，賣給五家補教業者。

系統入侵

*Source: 自由時報

超離譜 網售東森購物 8千筆個資

業者屋出包 卡號全都露 每筆5毛

2009年06月11日蘋果日報

新聞快訊 列印(37) 轉寄(0) 引用(0) 書籤

【郭睿誠、侯柏青／台中報導】八千筆東森購物台消費者個人資料在網路上「全都露」。有民眾周一在網路上宣稱「輸錢賣信用卡資料」，強調是「東森購物流出[redacted]分證字號等一應俱全[redacted]個檔案、多達八千筆免費資料供有意購買者參考。《蘋果》經抽樣訪問確認資料無誤。東森購物接獲《蘋果》查訪後表示已向警方報案；消基會則呼籲民眾慎選其他更安全的交易平台。

內部管控?

*Source: 蘋果日報

老師個資外洩 網站找得到

民視 (2009-05-30 15:55)

轉寄好友 友善列印

台中縣教育處不久前，彙整各校認輔老師的個人資料，結果100多位老師的個資卻不慎外洩，並且在中國知名網站，都能夠找到這些老師的個資，雖然網站已經把資料撤除，但老師們擔心，會讓有心人惡意使用。幾天前在中國的入口[redacted]縣的100多位認輔教師的個人資料，全都一覽無疑，原來是台中縣政府教育處，在資料傳輸時出了差錯，教育處承辦人員的疏忽，造成100多位老師的生日、身分證字號和住址等個人資料，在網路上曝光，老師擔心有心人利用個資犯罪。

未知原因

*Source: 新浪網

2009-3-21

4校長涉賣10萬學生個資

與補習班勾結 中彰廿多校受害

〔彰化小組／綜合報導〕校長爲錢，竟然出賣學生！彰化地檢署去年底接獲檢舉，指稱員林鎮大佳補習班涉嫌與多所學校校長、甚至前教育局長勾結，以現金行賄取得學生[redacted]縣市有二十多所[redacted]資被「賣」。

盜賣資料

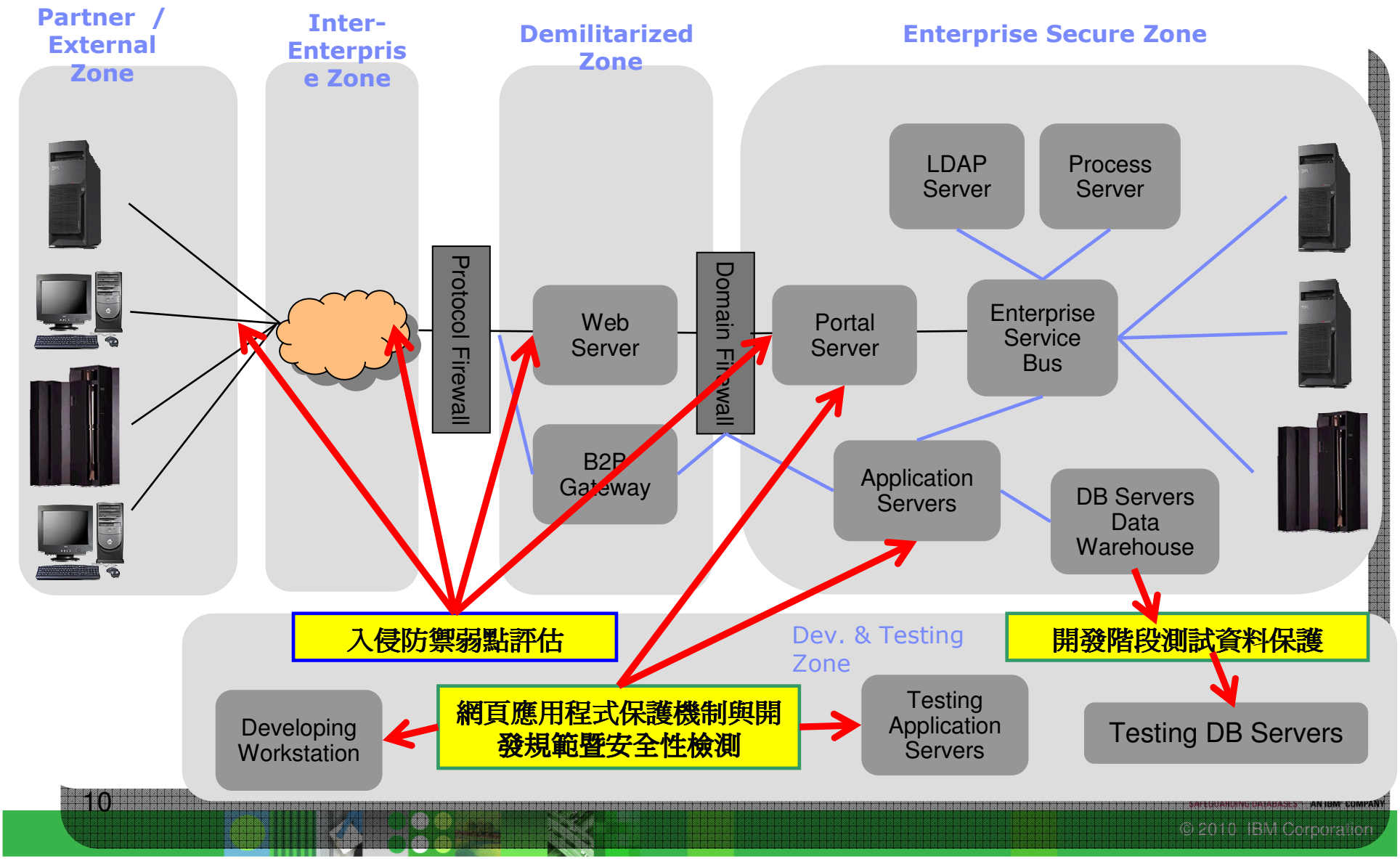
彰檢襄閱主任檢察官張慧瓊指出，檢方針對涉案重大的校長與業者展開監聽調查，今年二月初展開搜索約談，在主嫌吳芝庭（卅六歲）經營的大佳補習班搜到大批學生名冊與帳冊，吳芝庭坦承行賄校長，但因牽涉的學校過多，爲免吳芝庭串證或湮滅證據，將她收押至今。

市場調查揭示資料安全最大隱患來自於企業內部!!!

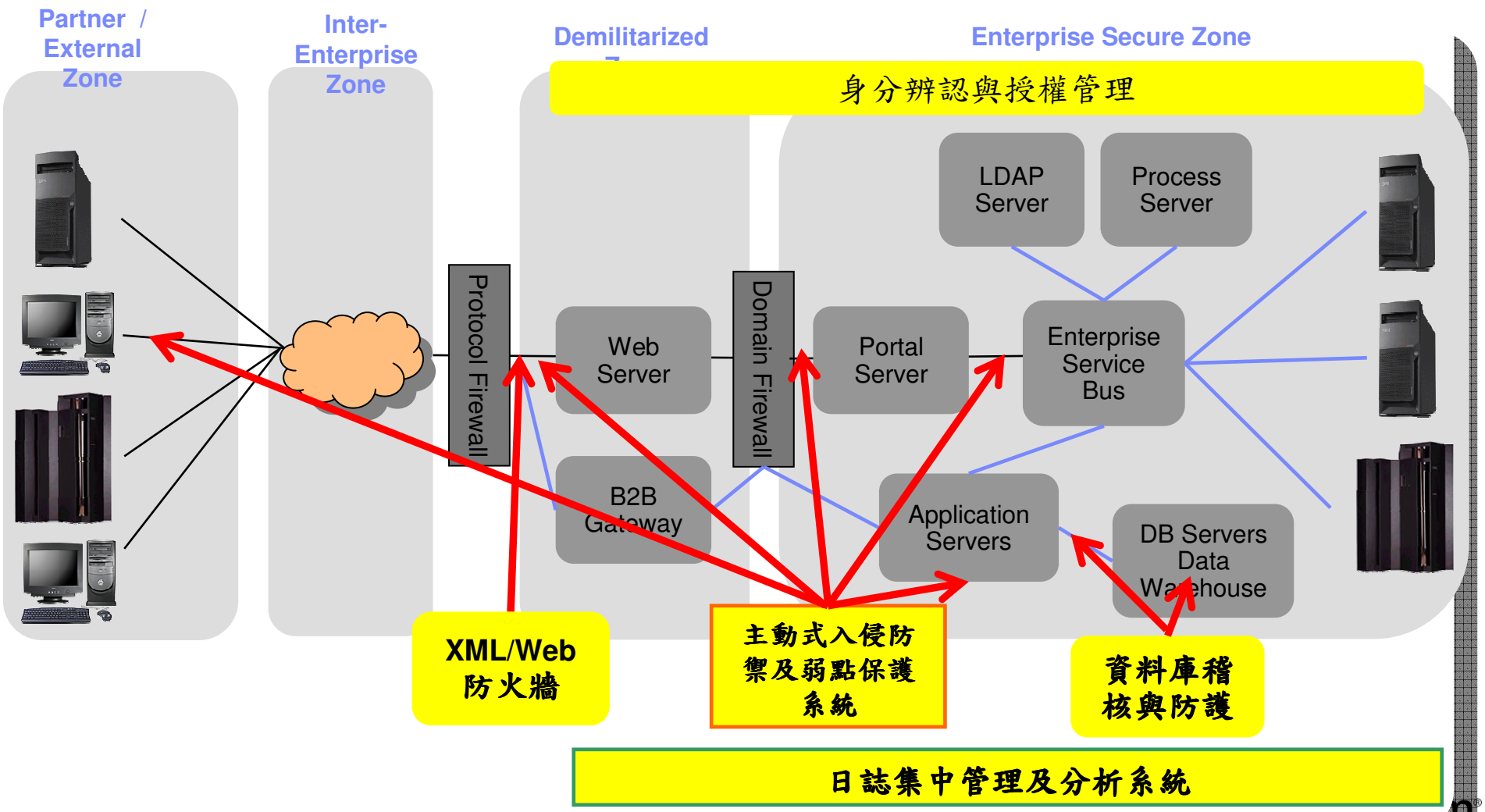
- 59%的受訪者承認離職後會帶走公司的資料；
- 79%的受訪者表示是在未經前雇主允許的情況下帶走公司資訊；
- 64%被員工帶走的資訊來自電子郵件；
- 被帶走的信息中有39%為客戶資訊，例如客戶聯絡方式；而有35%是員工資訊。
- 24%的員工在離職後仍然可以登錄公司的網路存取訊號；其中有35%的人在離職一周後仍然擁有這個許可權。

摘自:賽門鐵克與隱私及資訊管理調查機構(Ponemon Institute)共同發佈了一份以2008年離職員工為研究物件的調查報告

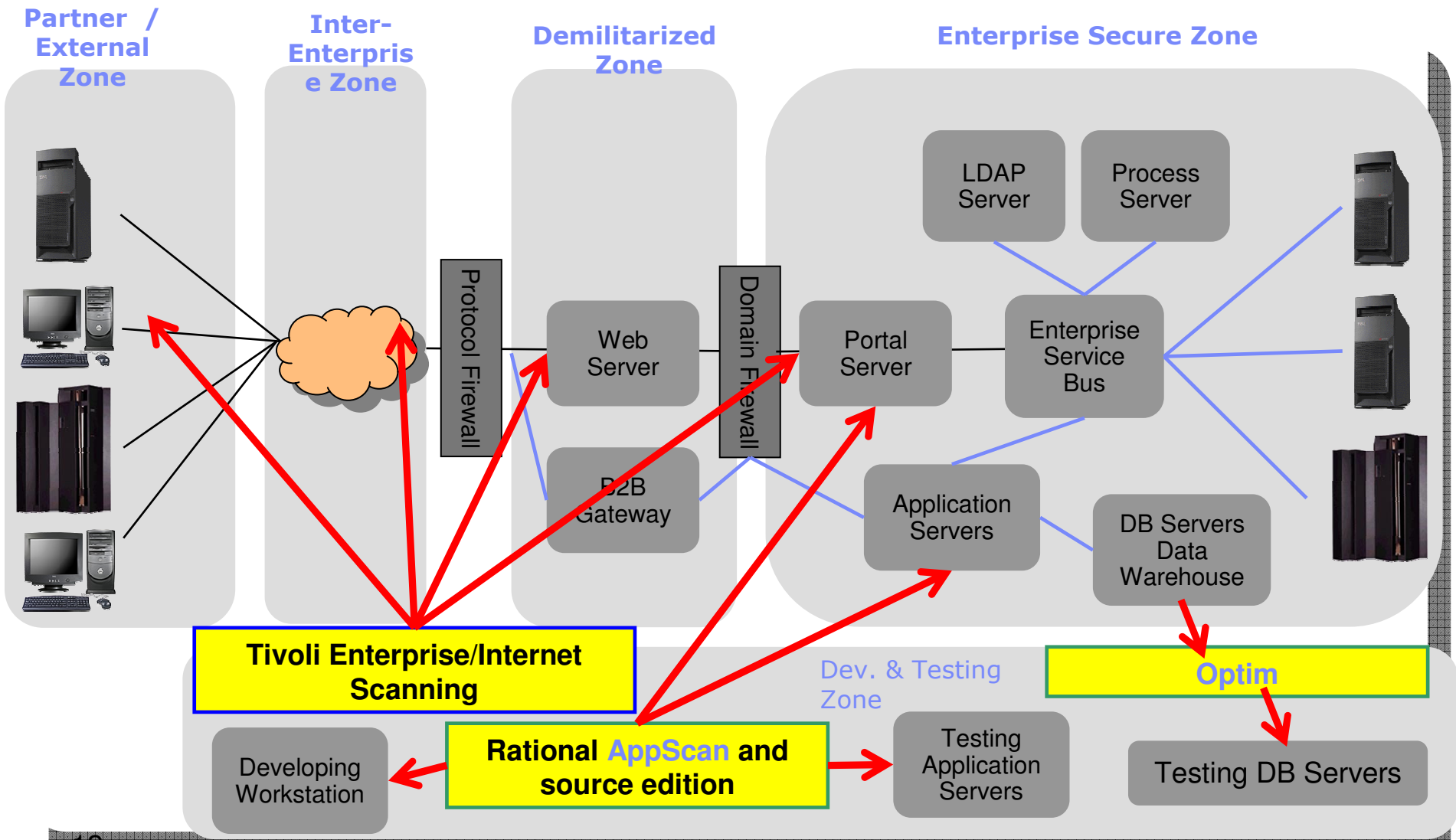
IBM資料安全解決方案實體架構圖–弱點評估與開發測試階段



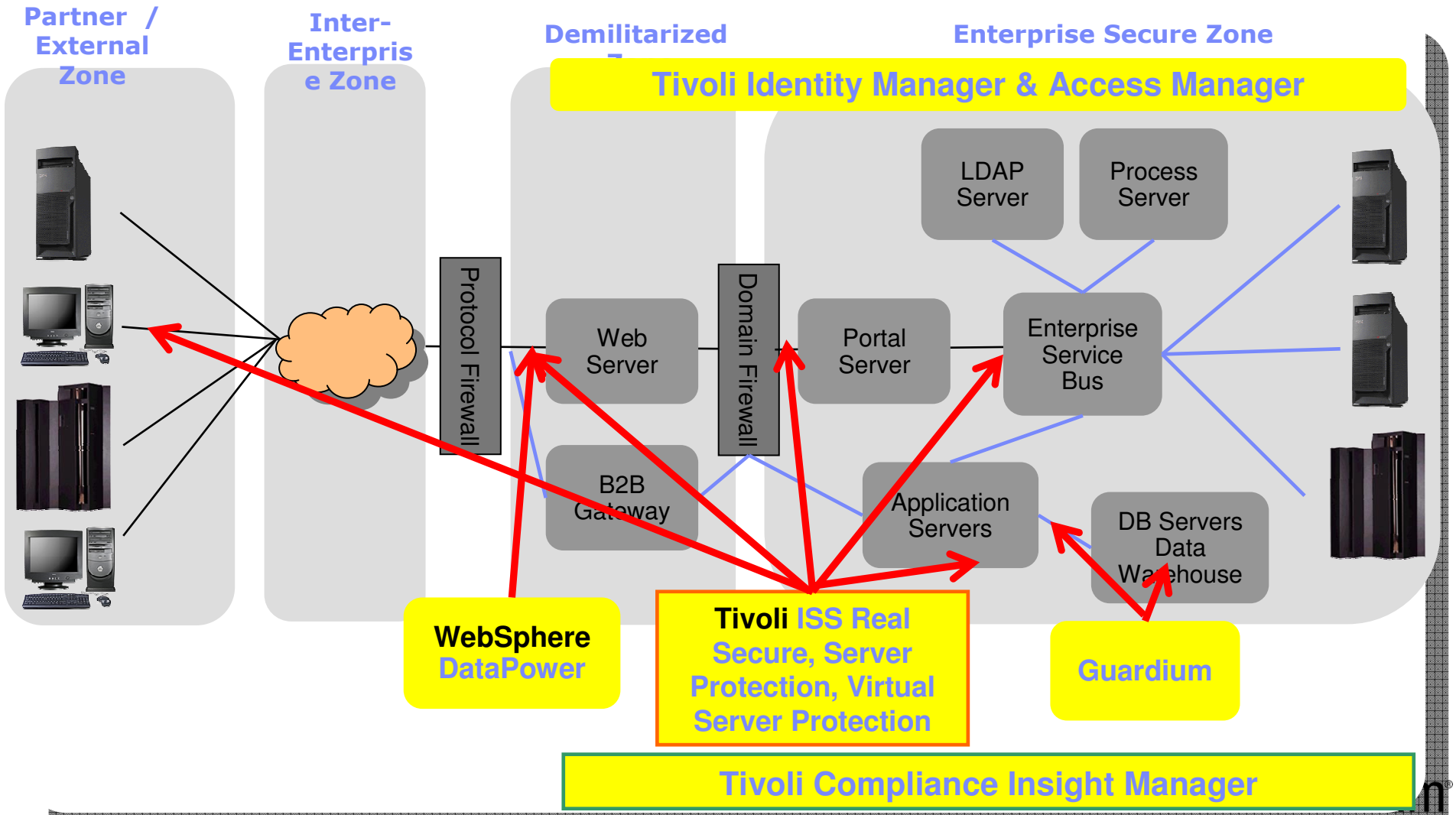
IBM資料安全解決方案實體架構圖 - 運行與維護階段



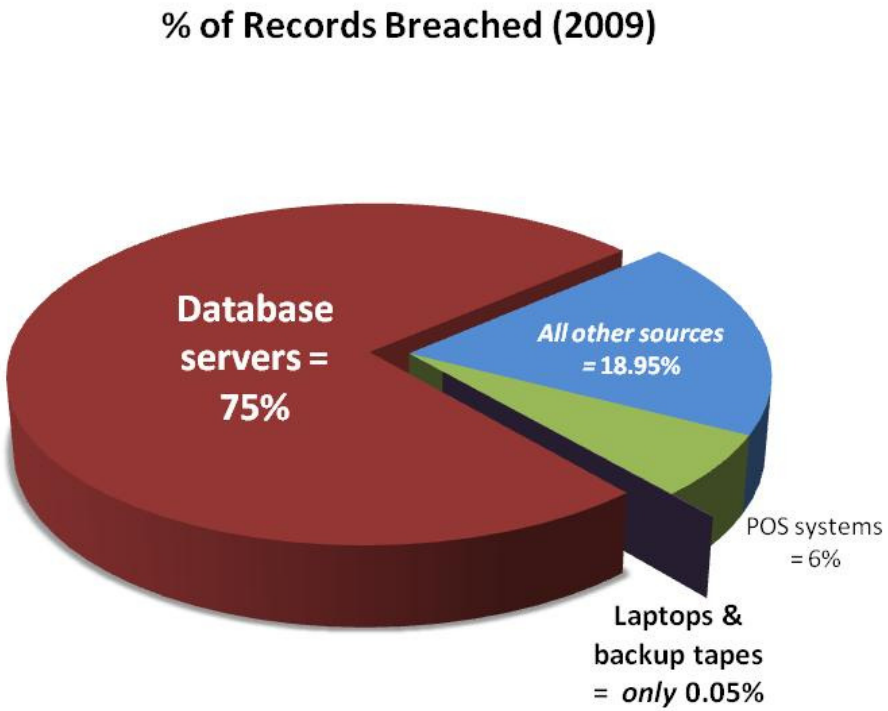
IBM資料安全解決方案實體架構圖–弱點評估與開發測試階段-軟體產品對應



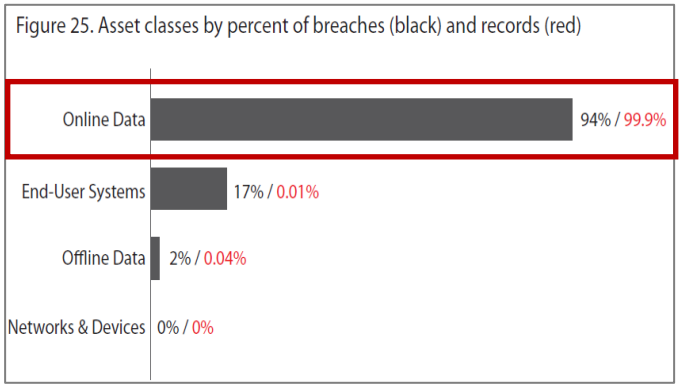
IBM資料安全解決方案實體架構圖 - 運行與維護階段 -軟體產品對應



資料外洩的來源...
Database Servers = Vast Majority of Compromised Records



Online data = 99.9% of all compromised records



"Although much angst and security funding is given to **offline data, mobile devices,** and **end-user systems,** these assets are simply **not a major point of compromise."**

2009 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

完整的資料庫安全生命週期

為何資料庫原生記錄(Native Logging)不適用

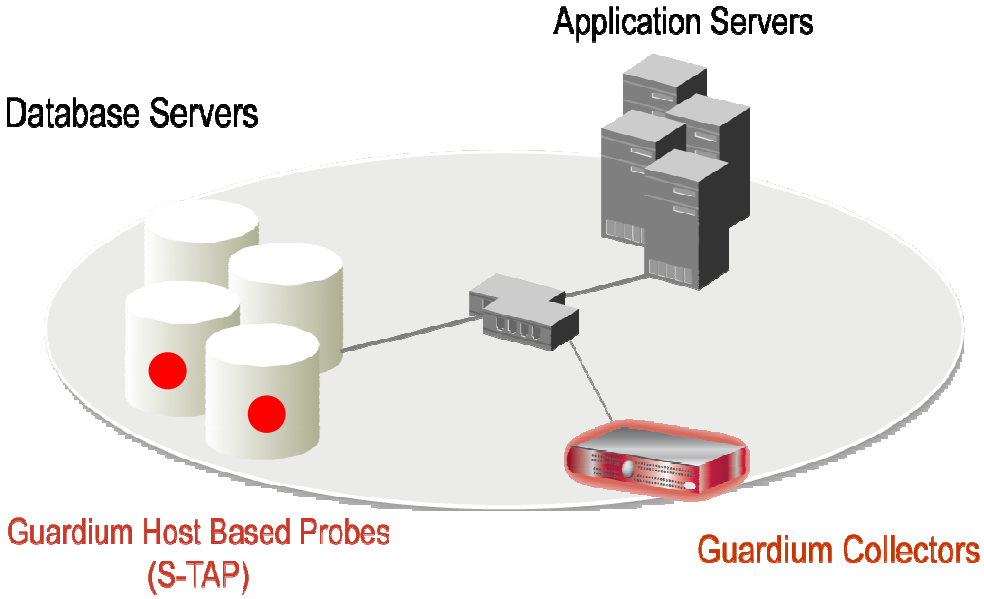
- 影響資料庫效能
  - Which table, from which IP, using which command, which program, …
- 非獨立作業 – 可以很容易被DBA關閉
- 跨資料庫平台會有不一致的稽核策略 (增加複雜度)
- 無法提供主動式的即時安全警示 (review logs every 3 months?)
- 在連接池(connection pooling)的環境無法確認應用程式端的使用者 (PeopleSoft, SAP, Oracle Financials, etc.) – potential fraud
- 須具有大量稽核資料儲存需求
- 在篩選稽核資料時，須撰寫程式
- 在產生符規的稽核報表時，須撰寫程式

成套裝置(Appliance) 與其它的解決方案有何不同之處?

- 即時安全警示與阻絕
  - 主動防護企業資訊
- 安全的稽核資料庫 (獨立作業)
- 詳盡的網路層級資訊
  - Client IP, OS login ID, source application, etc.
- 最小效能影響
- 不須變更資料庫或應用程式設定
- 具跨平台和企業層級的解決方案
  - 具稽核資料的彙總與正規化
  - 集中式的策略定義與執行能力

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium 解決方案
Real-Time Database Monitoring



ORACLE
IBM DB2
SQL Server
TERADATA
SYBASE
MySQL
Informix

- 細緻精密的策略與監控
  - *Who, What, When, hoW, Where*
- 即時警示
- 全面的活動監控包含本地端的存取
- 非侵入性
- DBMS獨立性
- 最小的系統影響(3 - 5%)
- 無需透過資料庫日誌和審計

Guardium提供深入的洞見...

- 誰正在對資料庫進行疑似異常的更動?
- 某些未經過授權的資料變更是在何時進行的?
- DBA或外包廠商對資料庫做了什麼更動?
- 已經發生了多少錯誤的登入紀錄?
- 誰正在擷取信用卡資料?
- 哪些資料正在被哪個網路節點存取?
- 哪些資料正在被哪個應用程式存取?
- 正在進行的資料存取使以什麼方式在進行的?
- 比對資料存取的時間, 是否有哪些可疑的模式?
- 資料庫正在產生什麼錯誤訊息?
- 誰在何時對資料庫進行疑似資料隱碼攻擊?

Guardium
AN IBM COMPANY

Guardium 提供包含下列解決方案

- **Real-time database activity monitoring (DAM)**
  - 資料庫即時監控(DAM)：主動地偵測與發現出未經授權認可，或可疑的資料庫存取活動。
- **Auditing and compliance solutions**
  - 稽核與制度方案：使各項資料隱私安全處理方法的導入，能更簡易地符合各項法規，如：SOX(美國沙賓法安 Sarbanes-Oxley)，PCI-DSS (支付卡產業之資料安全標準 Payment Card Industry Data Security Standard)。
- **Change control solutions**
  - 變更控制：在資料庫結構上、資料數值、特定者使用權、及系統設定上預防未經授權的變更。
- **Vulnerability management solutions**
  - 弱點安全管理方案：在弱點安全控管上的判讀及解決方案。
- **Database leak prevention**
  - 資料庫外洩防護系統：能指出在敏感的資料及對資料庫可能造成威脅的安全缺口，並加以防護。

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium通過行業專家的驗證

Validated by Industry Experts

FORRESTER®

"Dominance in this space"
#1 Scores for Current Offering, Architecture & Product Strategy

ChannelWeb

"Most Powerful Compliance Regulations

SC MAGAZINE

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security."

the 451 group

InformationWeek

"Top of DBEP Class
"Practically every feature you'll need to lock down sensitive data."

"Guardium is ahead of the pack and gaining speed."

"Guardium is ahead of the pack and gaining speed."

RED HERRING N. AMERICA WINNER 100

SQL SERVER MAGAZINE

2007 Editor's Choice Award in "Auditing and Compliance"

SECURITY MAGAZINE

"Enterprise-class data security product that should be on every organization's radar."

INFORMATION SECURITY Hotpick

Guardium
AN IBM COMPANY

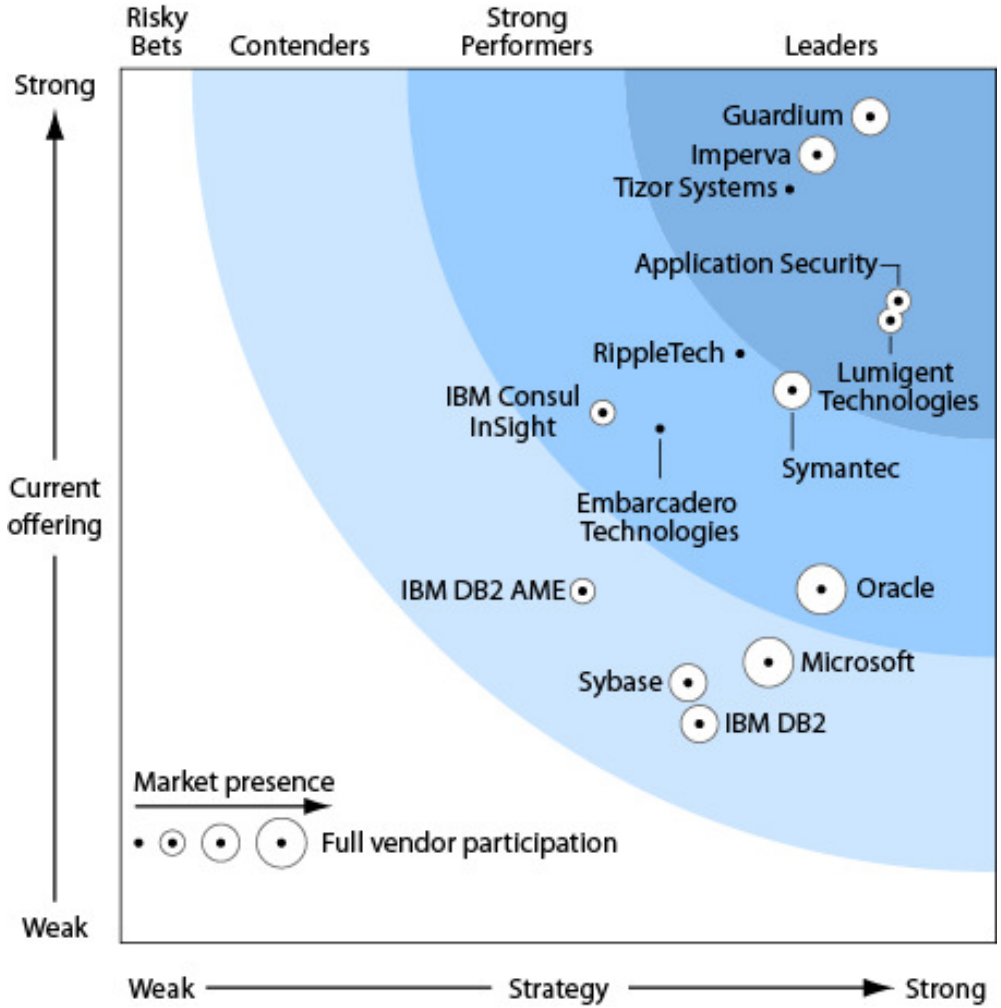
Information Management

FORRESTER

IBM

Highest Overall Score for Current Offering, Corporate & Product Strategy

- "Dominance in this space."
- "A Leader across the board."
- "Leadership in supporting large heterogeneous environments,… high performance and scalability, simplifying administration …and real-time database protection."
- "Strong road map ahead with more innovation and features."



Source: "The Forrester Wave™: Enterprise Database Auditing and Real-Time Protection

Guardium AN IBM COMPANY

全球領導企業均採用Guardium

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world's favorite beverage brands
- The most recognized name in PCs
- 15 of the world's leading telcos
- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

Guardium
AN IBM COMPANY

合規的工作
The Compliance Mandate

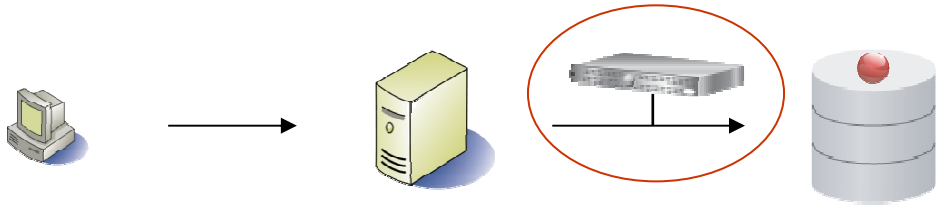
規定要求	CobiT (SOX)	PCI DSS	HIPAA	CMS ARS	GLBA	ISO 27002	NERC	NIST 800-53 (FISMA)
1.查詢敏感性資料 (Successful/Failed SELECTs)		✓	✓	✓	✓	✓		✓
2.改變表定義(DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓		✓	✓	✓	✓
3.資料操作 (DML) (Insert, Update, Delete)	✓			✓		✓		
4.例外操作 (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓	✓	✓	✓
5.授權變更(DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

Guardium AN IBM COMPANY

詳盡的稽核與安全

All SQL traffic contextually analyzed & filtered in real-time to provide specific information required by auditors



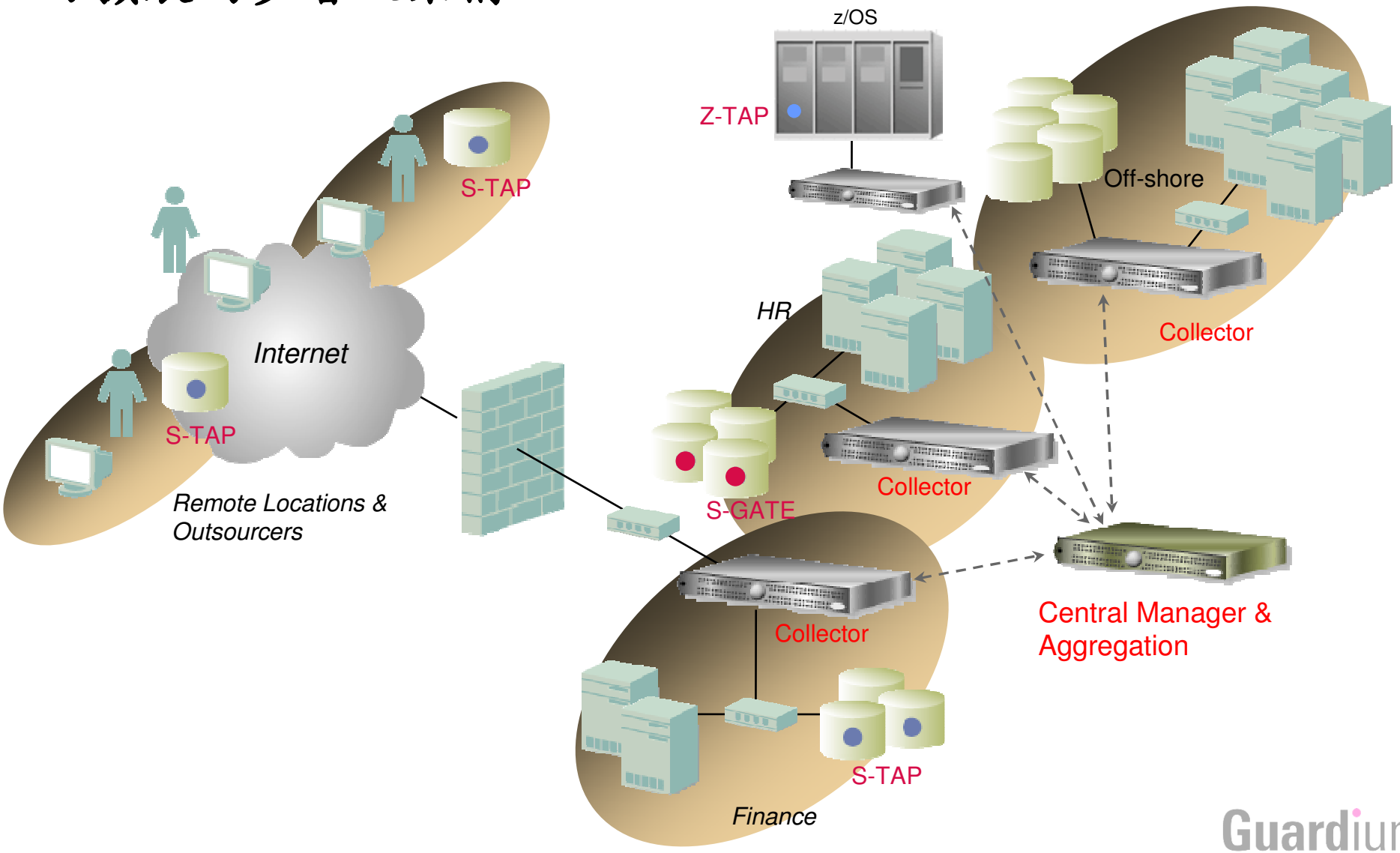
Client IP
Client host name
Domain login
Client OS
MAC
TTL
Origin
Failed logins

Server IP
Server port
Server name
Session
SQL patterns
Network protocol
Server OS
Timestamp
Access programs
App User ID

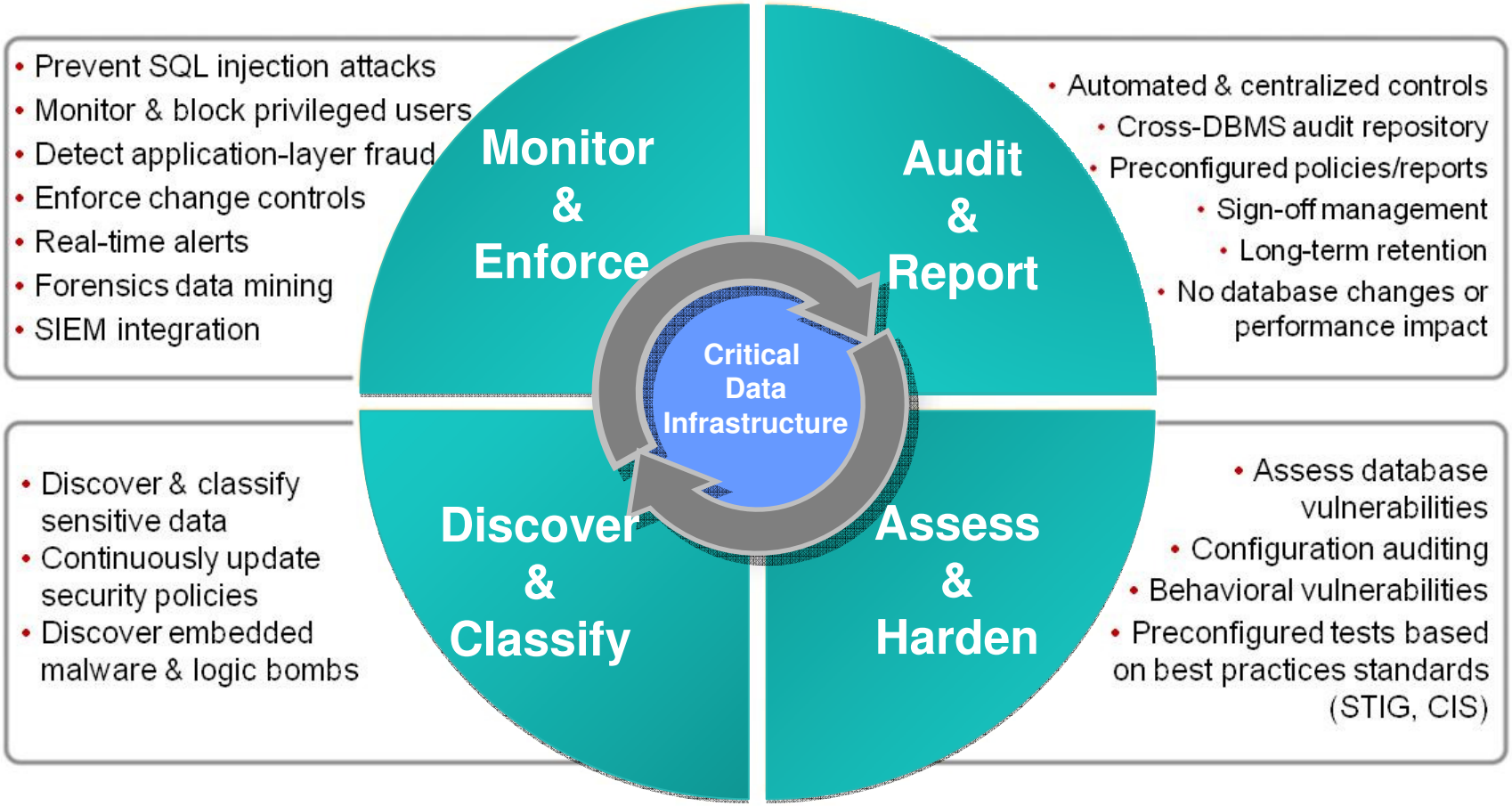
ALL SQL commands
Fields
Objects
Verbs
DDL
DML
DCL
DB user name
DB version
DB type
DB protocol
Origin
DB errors
SELECTs

Guardium AN IBM COMPANY

可擴展的多層次架構

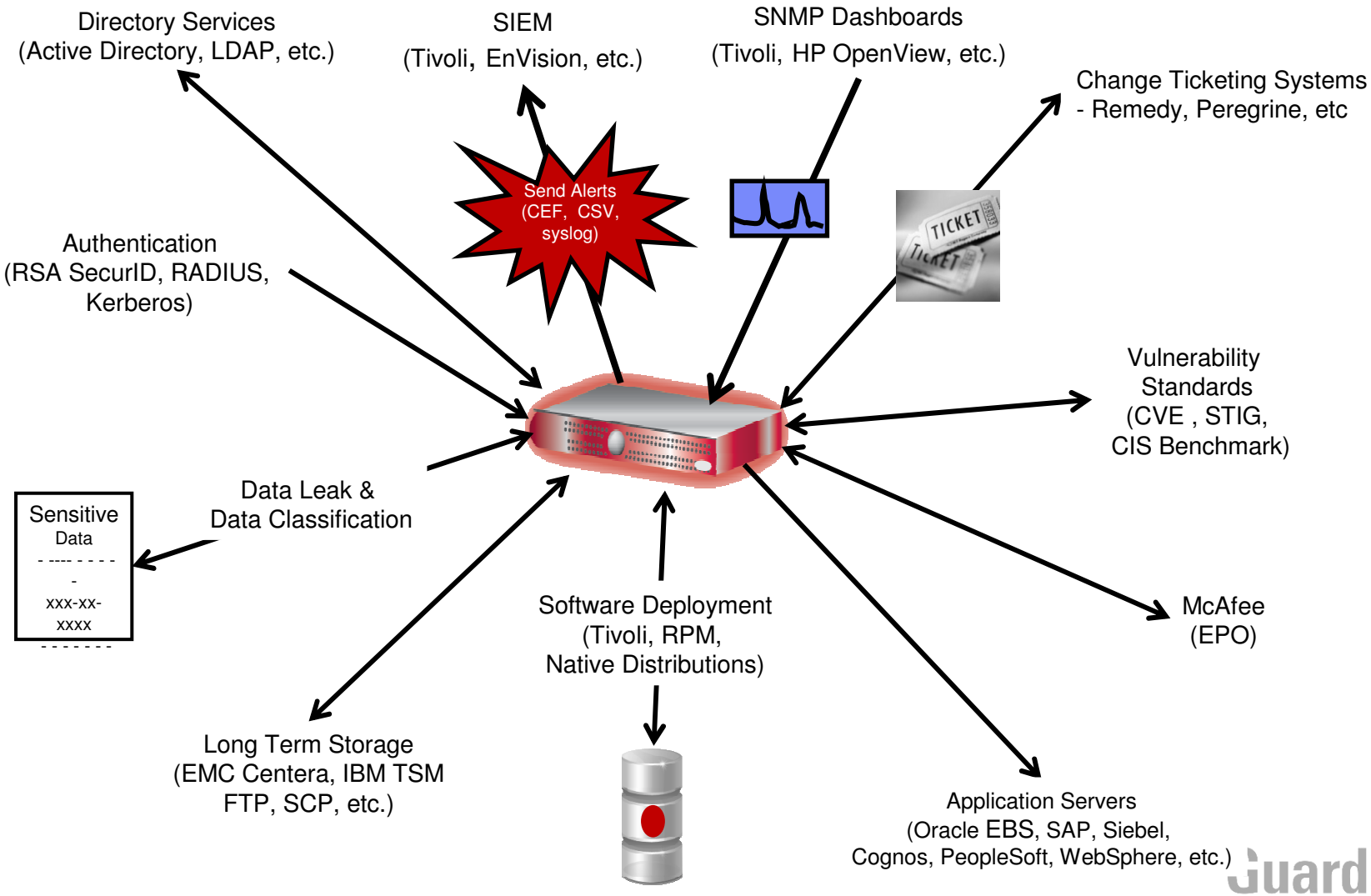


Guardium支援完整的資料庫安全生命週期



Guardium AN IBM COMPANY

與您現有的系統架構完全整合



Guardium 價值主張

- 確保企業資料的私密與完整
  - Enforce change controls & access controls for critical systems
  - Across entire application & database infrastructure
  - Oracle, SQL Server, IBM DB2 & Informix, Sybase, MySQL, Teradata
  - SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects, …
- 增加作業效率
  - Automate & centralize internal controls
  - Across heterogeneous & distributed environments
  - Rapidly troubleshoot performance issues & application errors
  - Highly-scalable platform proven in most demanding data center environments worldwide
- 不影響企業基礎架構或程序
  - Non-invasive architecture
  - No changes required to applications or databases

Guardium AN IBM COMPANY

Database Activity Monitoring (DAM) Supported Platforms

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UBD (Windows, Unix, z/Linux)	8.0, 8.2, 9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 UBD for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10,11
MySQL	4.1, 5.0, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02

Thank You!

Data Management

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY