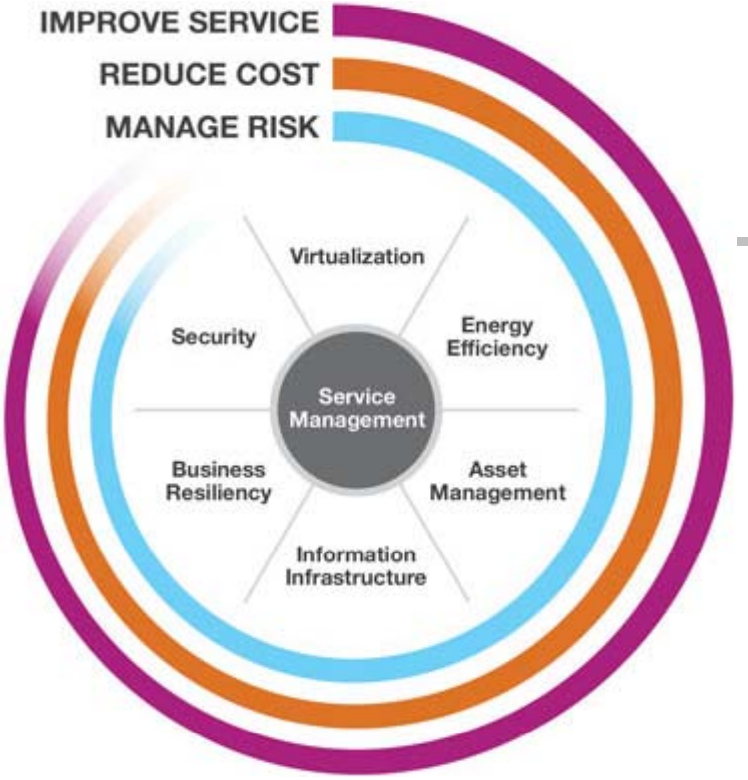
個資新時代下之企業個資新策略分享

擘畫個資安全新藍圖 讓企業攻守俱佳



林育震 Julian Lin
台灣IBM技術總監
0932-035660
julin@tw.ibm.com

A Smarter Planet

SmarterSecurity&Resilience

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 新版個資法之內容定義及企業衝擊分析
- IBM協助解決方案簡介
- IBM協助解決方案舉例

國內的個資外洩問題不斷且常成為媒體焦點，且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[illegible]數加密電子檔等，還與主辦的國立桃園高級中學簽定「[illegible]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

2009-3-21

*Source: 自由時報

超離譜 網售東森購物 8千筆個資

業者屢出包 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[illegible]分證字號等一應俱全[illegible]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

Ads by Google
Branding Taiwan 短片競賽 Youtube.com/TaiwanExcellence
發揮你的創意,以5分鐘短片呈現台灣產業風貌,向世界發聲,還有機會拿獎金!

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[illegible]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

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[illegible]縣市有二十多所[illegible]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。

個資洩漏的相關統計資訊及研究報告：主要事件來源

個資洩漏事件，最主要可粗分為下列幾種事件來源：

節點防護不足

- 筆記型電腦或個人電腦的遺失或被竊取
- 遺失或被竊取的儲存媒體

未有整體防禦架構

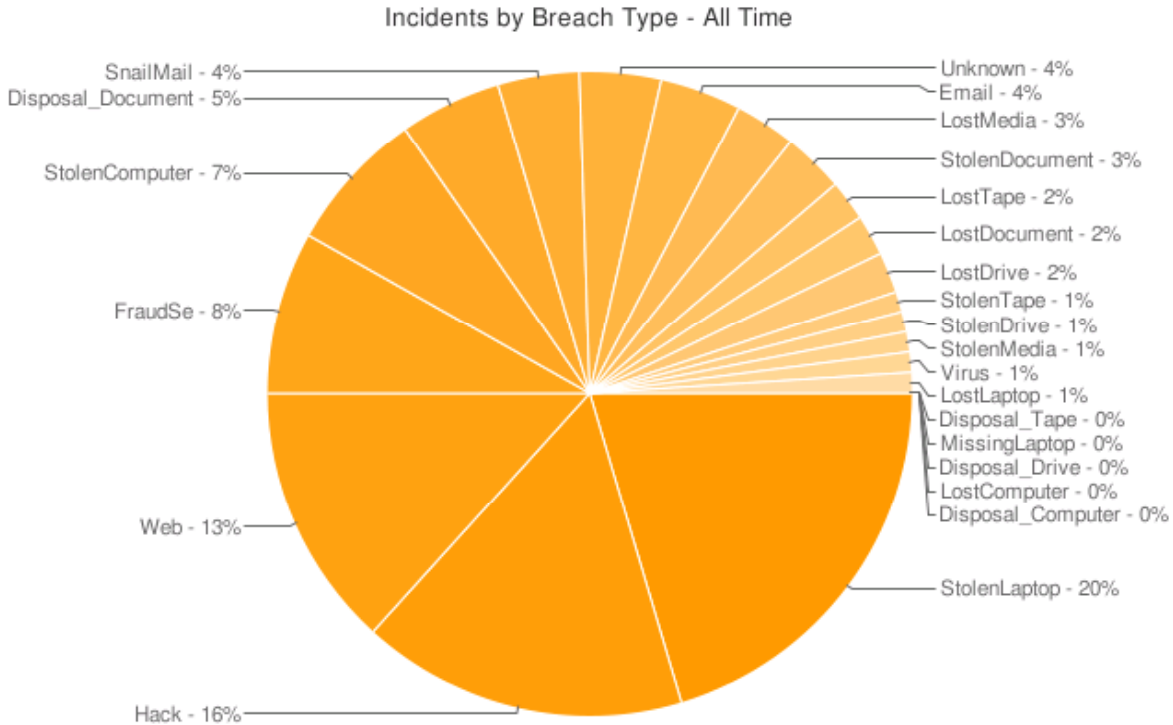
- 外部駭客攻陷Web應用程式或資料庫，抓取個資

缺乏資料運用政策

- 惡意的高權限內部系統管理者或維護廠商

未具備資料外洩處理分析能力

- 惡意的內部使用者



Source: DataLossDB, Open Source Foundation

新版個資法的實施時程及範圍

- 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年十二月開始施行 (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

個資法最新定義及適用情形

第二條 本法用詞，定義如下：

1. 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。
2. 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。
3. 蒐集：指以任何方式取得個人資料。
4. 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。
5. 利用：指將蒐集之個人資料為處理以外之使用。
6. 國際傳輸：指將個人資料作跨國（境）之處理或利用。
7. 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。
8. 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）
9. 當事人：指個人資料之本人。

新版個資法對企業的主要影響簡介

- 公務機關及非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏
- 非法變更、刪除個人資料致妨害正確性足以損害個人時: 五年以下、一百萬以下罰金之之刑責
- 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

除了個資外，各行業都有營業秘密資料，如：製程流程與參數、財務資料、IC設計資料 …。而且從外部入侵或在內部盜取都可能發生

行業別	營業秘密	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、物流行業網路商店	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

不論個人資料或是營業秘密都可以用同樣的技術來保護

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 新版個資法之內容定義及企業衝擊分析
- **IBM協助解決方案介紹**
- **IBM協助解決方案舉例**

資料安全的整體架構必須是全面性的考慮：客戶需全面且整體性重新檢閱資料散佈情形、建立資料的資產管理機制、評估各項資料的外洩風險、依據風險高低運用「機制、工具或監控」等方式達到管理目標

一般而言，企業面對個資法可採取的因應措施大致可分為兩大方向：

1. 評估個資外洩的風險
2. 建立符合需求的個人資料保護系統

在評估個資外洩風險時，需瞭解個資外洩主的可能管道：
外部入侵、委外廠商洩漏、內控程序疏失，以及內部人員洩漏等

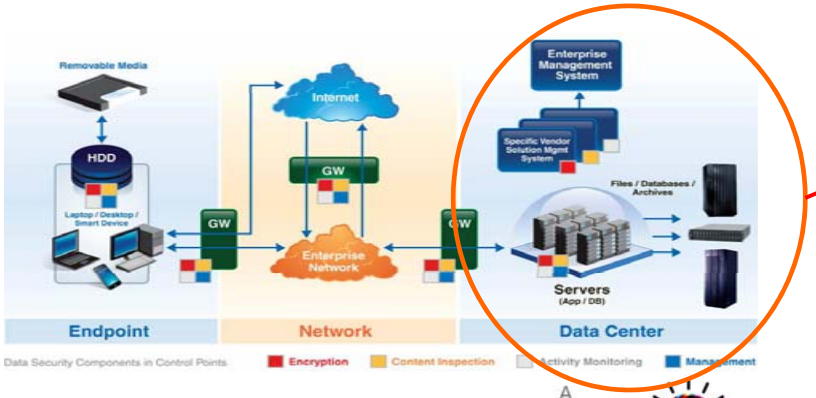
but

如何開始?

在建立符合規範的個人資料保護系統時，也要先了解個人資料處理的流程：

1. 蒐集階段，要依法進行告知義務並取得書面同意
2. 其次是處理，採取適當保護措施避免個人資料被竊取、竄改或毀損
3. 利用階段，客戶資料必須依蒐集時的特定目的範圍內才可使用，（如果要在範圍外使用，必須另外取得書面同意。）
4. 最後是銷毀，這也是最容易被企業忽略的階段，如果蒐集資料時的目的消失了，或期限屆滿，企業必須將資料完全銷毀。

也必須考量個人資料處理的含括面向：
移動式儲存媒體、個人處理節點、
網路、應用系統、資料庫、
伺服器以及儲存體等

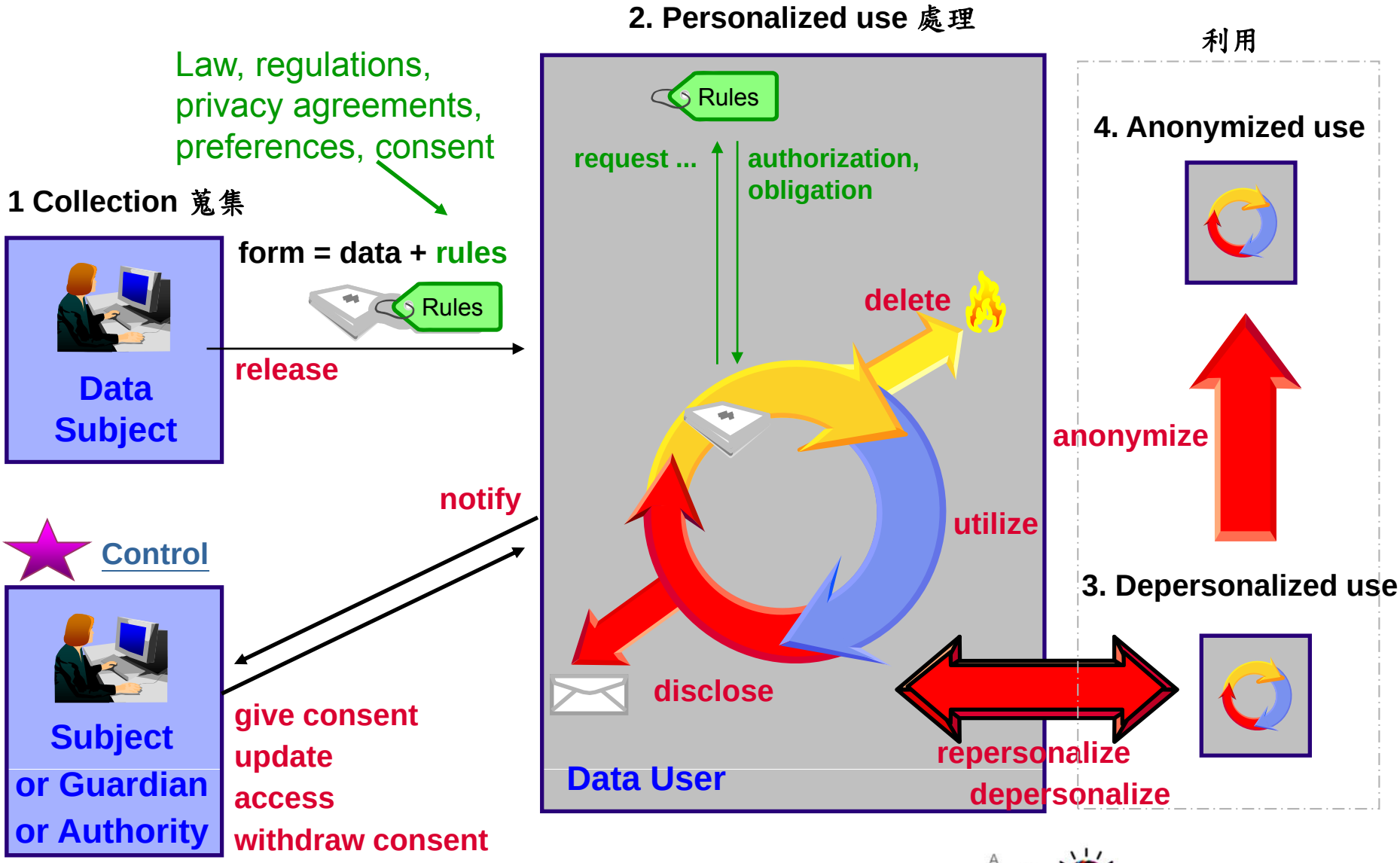


伺服器端最重要

A Smarter Planet

SmarterSecurity&Resilience

個人資料/營業祕密之生命週期防護架構參考



每當新科技問世，機會與風險之間的界線便會些許挪移。在我們積極探索新技術所蘊含的機會與潛能的同時，有心人士也急於鎖定弱點發動攻擊。因此，隨著科技推陳出新，組織因應安全威脅的策略也可能產生根本的改變。

新興科技的推陳出新

MILS VPN Laptop Encryption SOX Physical Access IPSEC DAC HIPPA SSL SAML Identity Management Password Smart Card PCIDSS MLS SaaS Token FIPS 140-2 Biometrics Trusted Computing XML Gateways PKI Cross Domain Systems Kerberos Thin Clients Accreditation H/W Crypto Digital Certificate Trusted OS LSPP/EAL4+ MAC Guards Hardening SABI/TSABI Wireless Secure Blades Tripwire Secure Collaboration Cyber Security Federation TCP Wrapper Cloud RSBAC FISMA Compliance SOA Security

1

* Not a complete collection

科技驅勢所帶來企業運作的安全挑戰


即時感應實體資產安全防護


捍衛行動裝置及個人資訊設備


保障網絡安全


應用程式運用安全可預測性


資訊安全及隱私


管理風險及法規需求

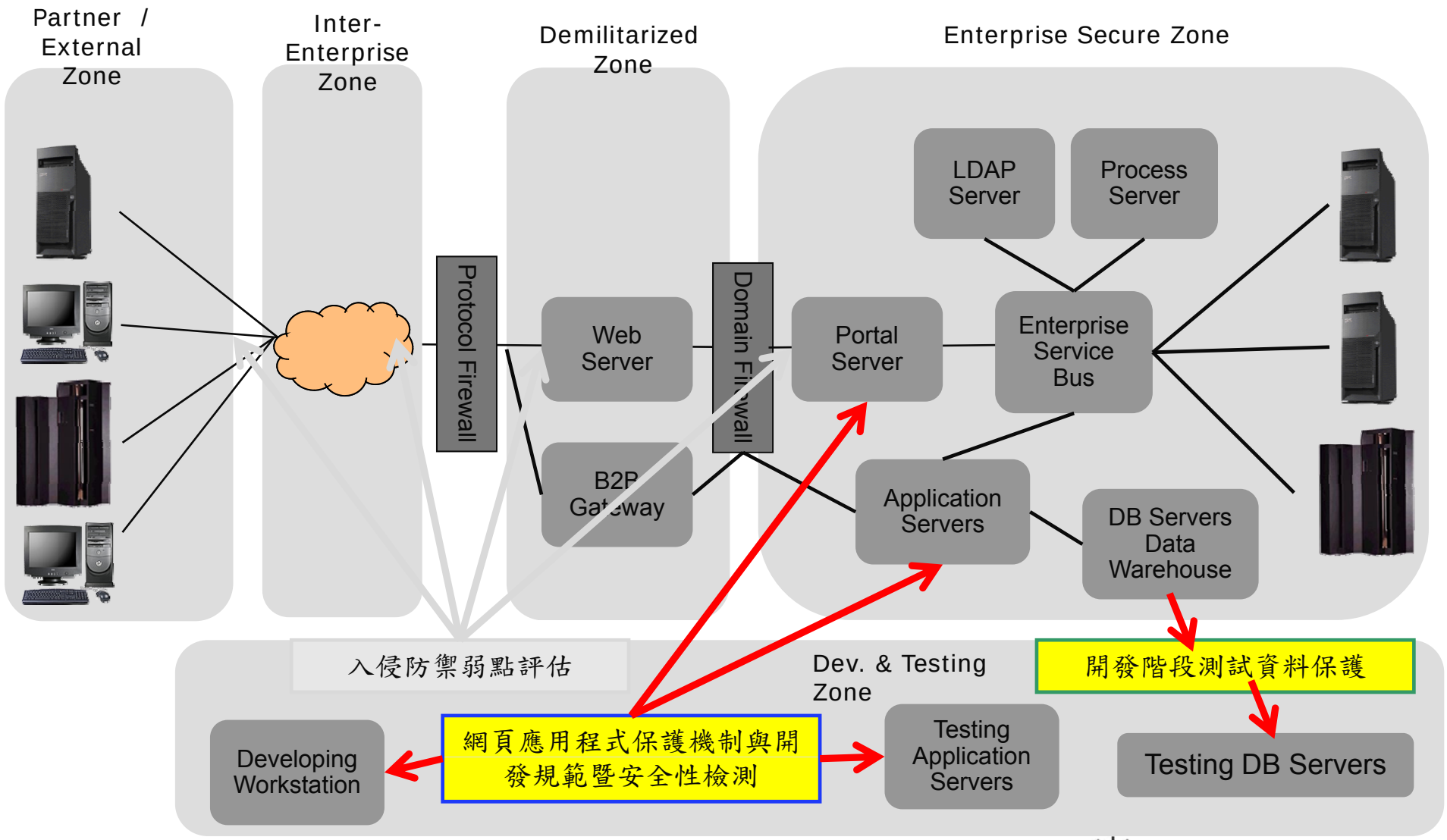
A Smarter Planet

SmarterSecurity&Resilience

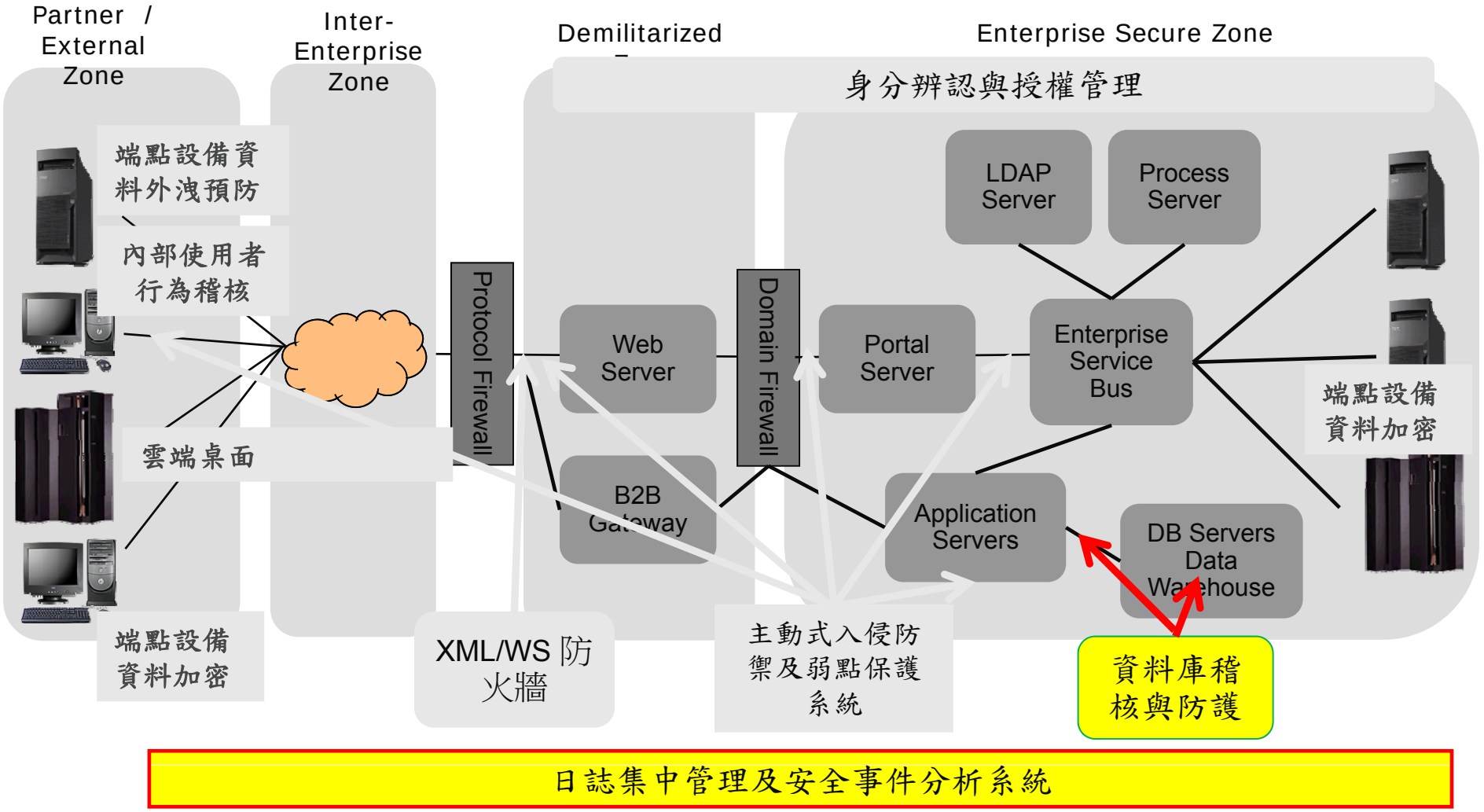
因應『新版個資法』的 法規要求及對IT系統影響；IBM從資料處理流程的控管角度 ，針對所涉及三大IT議題，提出因應方針及相關流程整合 解決方案。完整包含顧問服務、軟硬體系統

法規要求	IBM解決方案套餐	IBM 解決方案	產品與服務對應
個資法	風險與弱點評估 制訂資安及隱私政策	■ 個資文件與資料分類分析與保護政策的訂定 ■ 制定個人資料保護政策並進行隱私資料流分析	■ GTS consultant ■ GTS consultant
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	資料運用與保護	■ 入侵防禦弱點評估諮詢與設計服務 ■ 隱私與測試資料保護弱點評估諮詢與設計服務 ■ 網頁應用程式保護機制與開發規範暨安全性檢測服務 ■ 主動式入侵防禦及弱點保護系統規劃與建置服務 ➢ XML/ WS 防火牆規劃與建置服務	■GTS + Tivoli ISS Enterprise Scanner ■GTS + **IM Optim** ■GTS + **Rational AppScan** ■GTS + Tivoli ISS IDS/IPS ■GTS + WebSphere DataPower
	節點資料洩漏保管	■ 端點設備資料外洩預防規劃與建置服務 ■ 資料加密規劃與建置服務 ■ 磁帶端點設備機加密與保管解決方案 ■ 雲端桌面資料保護解決方案	■GTS service (Digital Guardian) ■GTS service ■STG tape drive, library ■GTS service (desk top cloud)
資料外洩損害賠償， 非公務機構需證明「無故意或過失責任」，才能免責	資料外洩分析與處理	■ 內部使用者行為稽核規劃與建置服務 ■ 資料庫稽核與防護系統規劃與建置服務 ■ 日誌集中管理及安全事件分析系統規劃與建置 ■ 身分辨認與授權管理規劃與建置服務	■GTS service (Intellinx) ■GTS + **IM Guardium** ■GTS + **Tivoli SIEM** ■GTS + Tivoli Identity Mgmt, Access Mgmt

IBM資料安全解決方案實體架構圖－評估弱點風險與開發測試階段



IBM資料安全解決方案實體架構圖 – 運行與維護階段



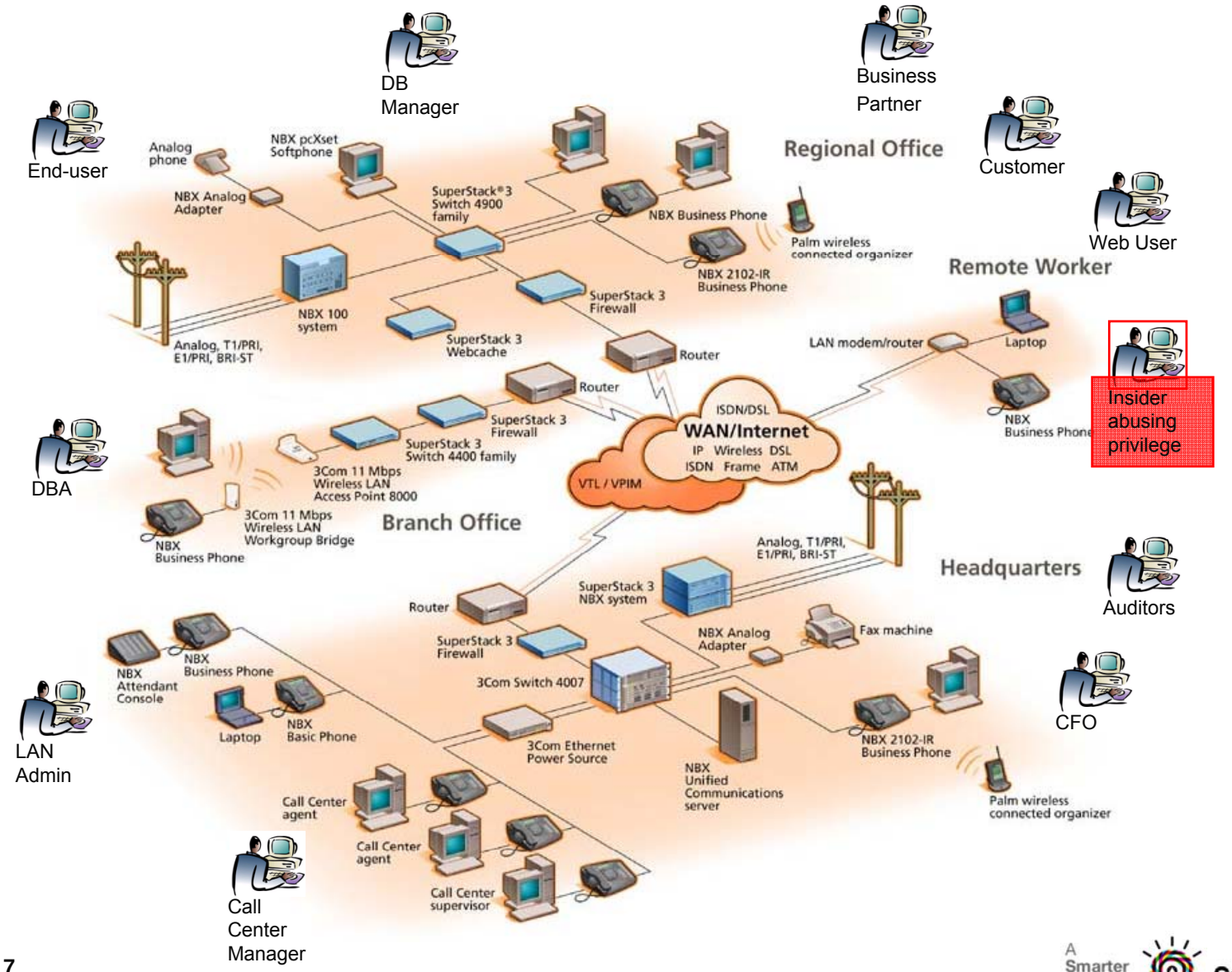
Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 新版個資法之內容定義及企業衝擊分析
- IBM協助解決方案介紹
- **IBM協助解決方案舉例**
  - 日誌集中管理及安全事件分析
  - 資料庫稽核與防護
  - 隱私與測試資料保護
  - 網頁應用程式保護機制與開發規範

有哪些使用者在你的網路中做什麼事? 您如何稽核?



安全問題:

1. 十個最大的企業安全問題中的三個是和內部安全相關的:
   - 雇員安全
   - 資料被合作夥伴/雇員偷取
   - 內部破壞
2. 美國企業每年由於內部欺騙導致損失超過600億

端到端的稽核 - 日誌集中管理及安全事件分析的挑戰、開發與測試的挑戰

•有沒有辦法從系統、應用程式、資料庫或網路層面的日誌進行追蹤？

- 是否有人對敏感資料進行了不當地使用或修改？（使用制度）
- 外包企業是否負責任地管理著系統和資料？（變化管理）
- 是否存在非法修改操作環境的情況？（變化管理）
- 如果有人新增使用者帳戶，我們能否收到告警？（帳戶管理）
- 是否定期記錄並審核系統管理員和系統操作人員的行為？
- 是否記錄下了所有的敏感資料存取活動 – 包括超級使用者/管理員和 DBA 的存取記錄？
- 是否對安全事故和可疑行為進行了分析和調查並採取了補救措施？
- 誰在未得到許可的情況下擅自終止了主要系統進程的運行？
- 管理員是否曾在系統中創建並批准創建特殊身份/特權？

- 測試資料、分析統計資料等會不會洩漏個資？一定要用原始資料嗎？
- 如何防範於未然？讓我的應用系統沒有漏洞？

資料源的稽核 - 資料庫稽核與防護的挑戰 who, when, what, which, how…

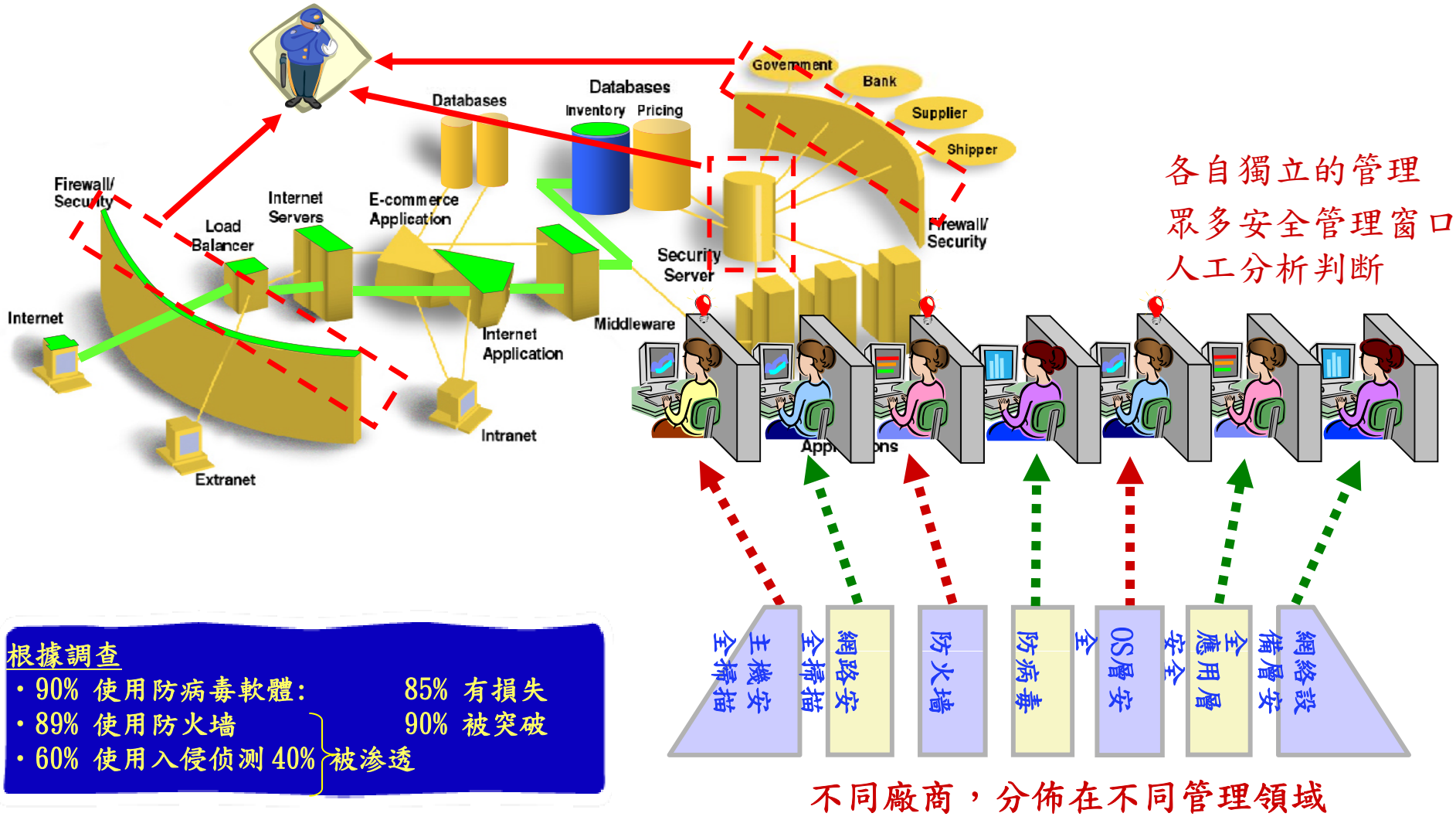
Table 9. Detailed listing of compromised assets by percentage of breaches and records

Asset	Asset Group	% of Breaches	% of Records
POS system	Online Data	32%	6%
Database server	Online Data	30%	75%
Application server	Online Data	12%	19%
Web server	Online Data	10%	0.004%
File server	Online Data	8%	0.1%
Public kiosk system	Online Data	2%	0.4%
Authentication / Directory server	Online Data	2%	0.1%
Backup tapes	Offline Data	1%	0.04%
Documents	Offline Data	1%	0.000%
Workstation	End-User System	8%	0.01%
Laptop	End-User System	4%	0.000%
PIN Entry Device	End-User System	2%	0.004%

Source: 2009 Data Breach Report from Verizon RISK Team

- 誰正在改變資料庫結構或刪除資料表?
- 何時有未授權的程式正在改變資料?
- DBAs 或外包維護人員正在對資料庫作什麼事?
- 有多少未成功的系統登入發生?
- 誰正在擷取信用卡資料?
- 什麼資料正在被網路上的哪個節點所存取?
- 什麼資料正在被哪個應用程式所存取?
- 這些資料是如何被取得的?
- 這些日子來資料被取得的行為模式有哪些?
- 資料庫產生了什麼錯誤訊息?
- 敏感性物件的暴露風險是什麼?
- 何時有人發動了資料隱碼攻擊?

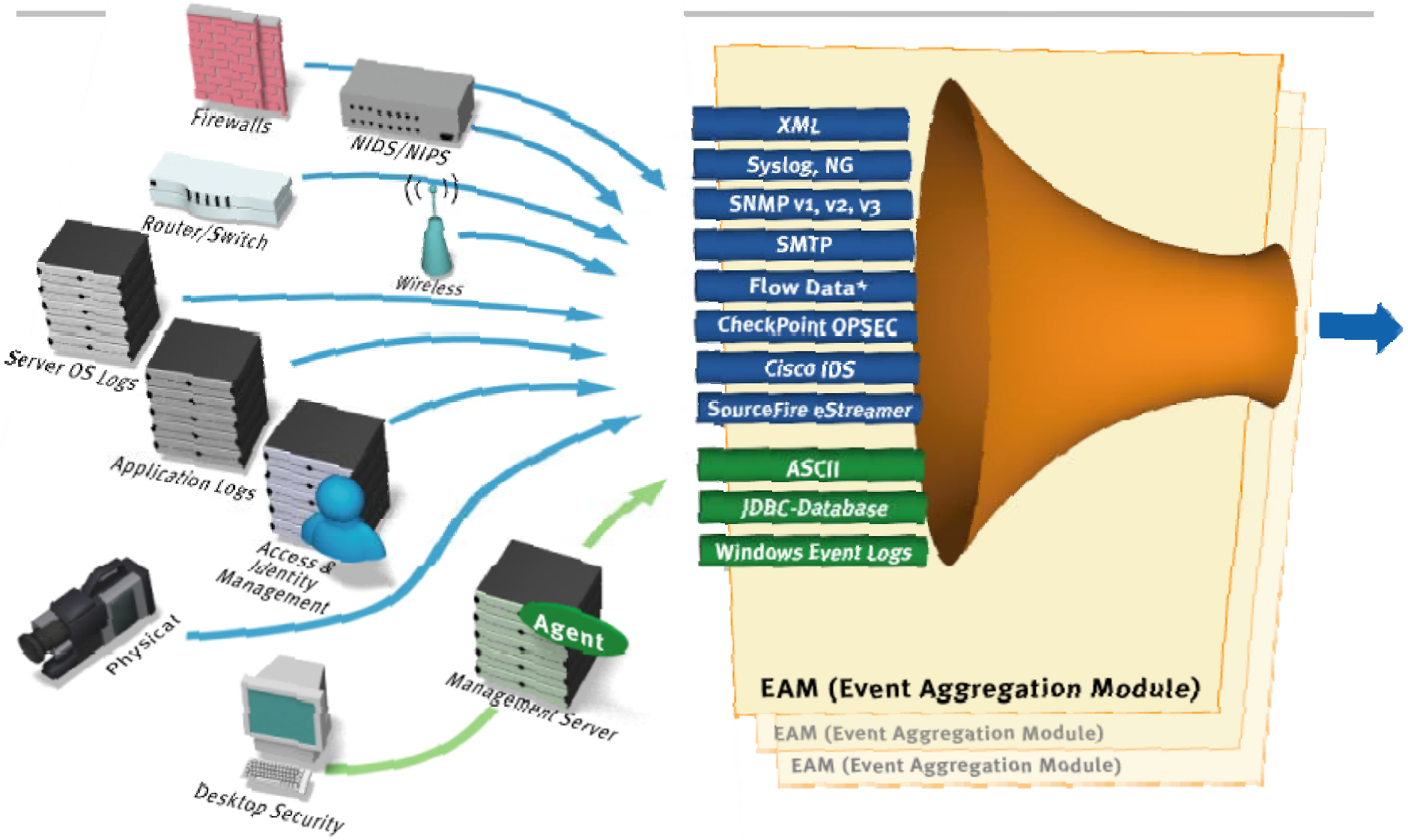
稽核與分析內部使用者行為之外，散布在各地的安全防護是否有達成預定的效果？是否能端到端綜合分析，證明已善盡保管人責任，並且找出問題點在哪裡發生



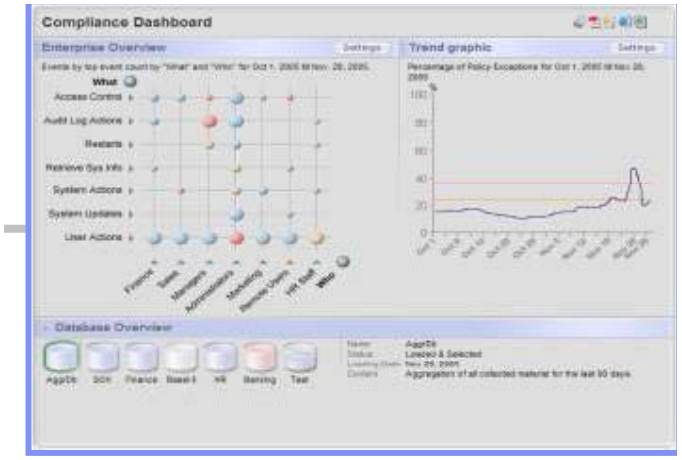
根據調查

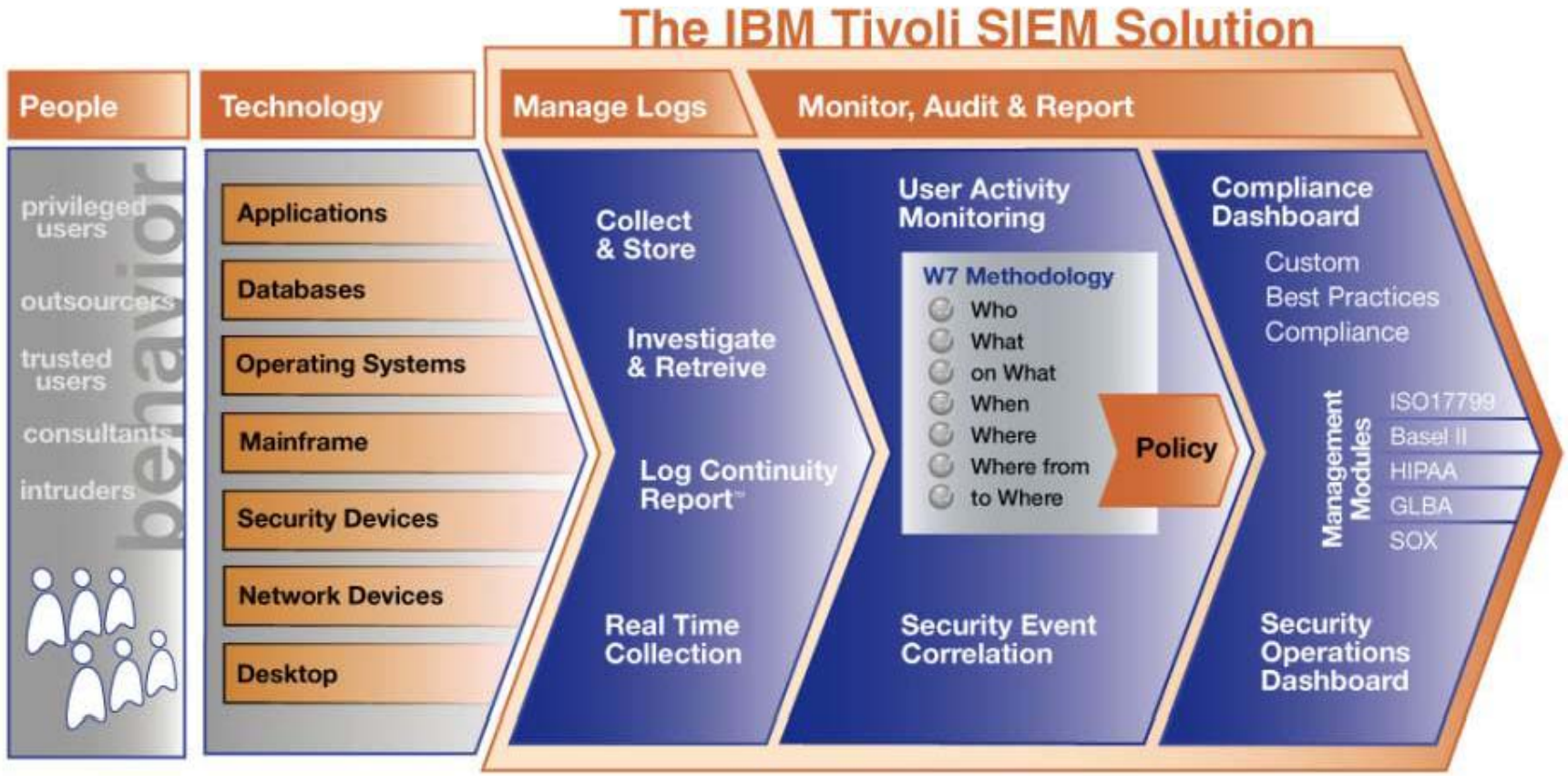
- 90% 使用防病毒軟體: 85% 有損失
- 89% 使用防火墻 90% 被突破
- 60% 使用入侵侦测 40% 被滲透

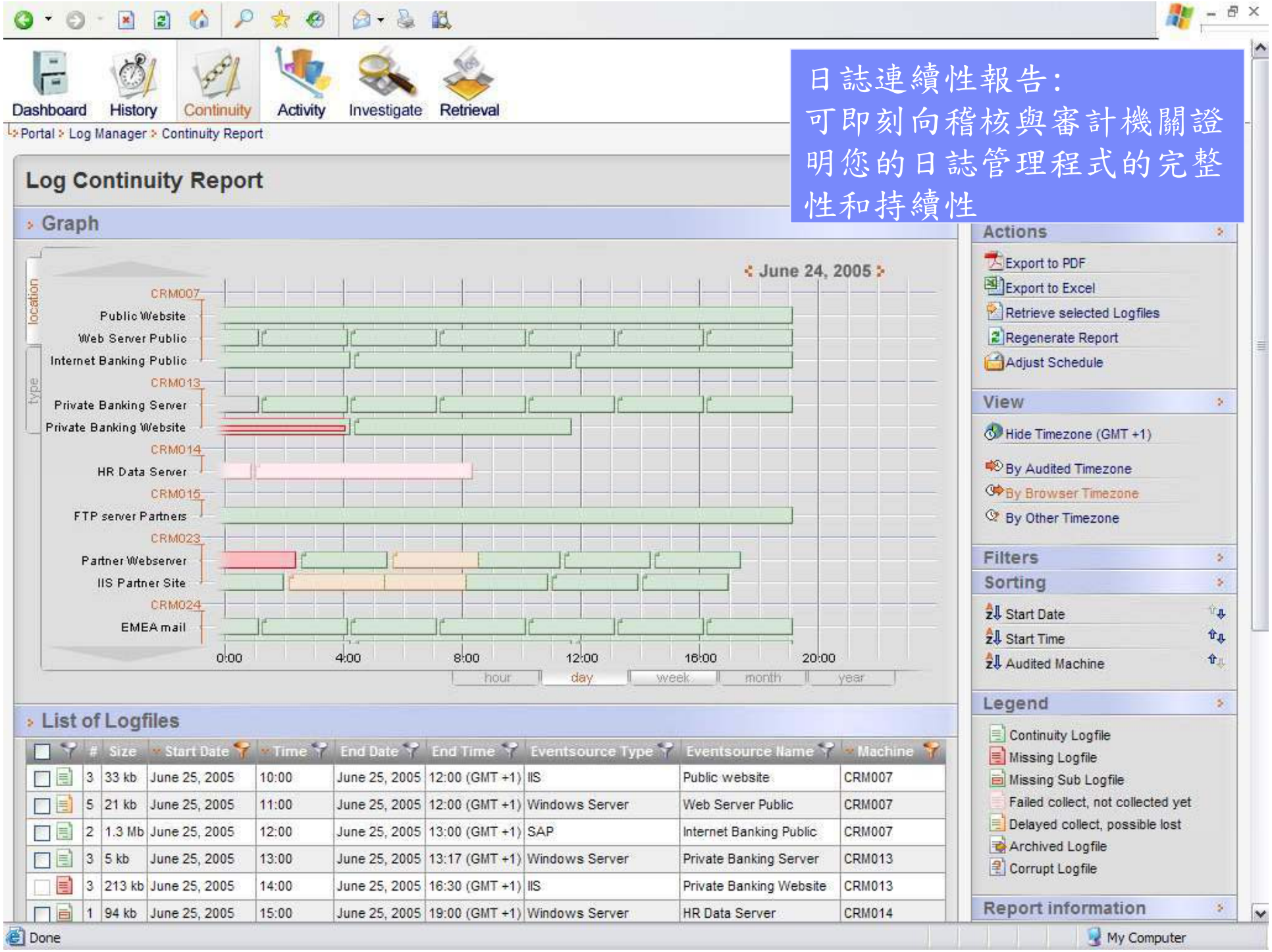
IBM日誌集中管理及分析方案提供廣泛的安全事件即時收集與分析



IBM日誌集中管理及分析方案能收集Desktop、Network Devices、Security Devices、mainframe、OS...等的日誌，將安全事件關聯起來，產生各種合規報表，並隨時反映在儀表板上

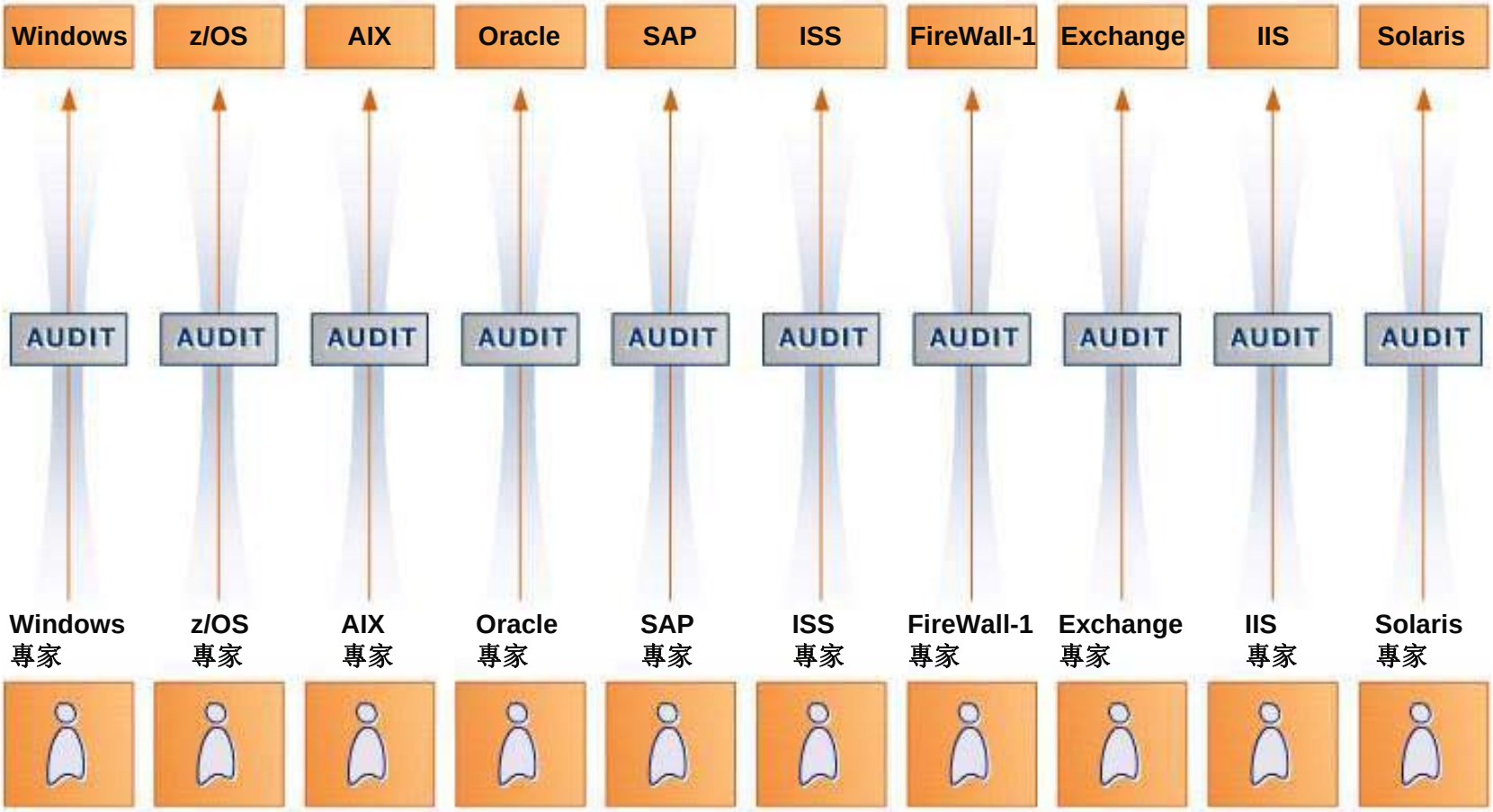






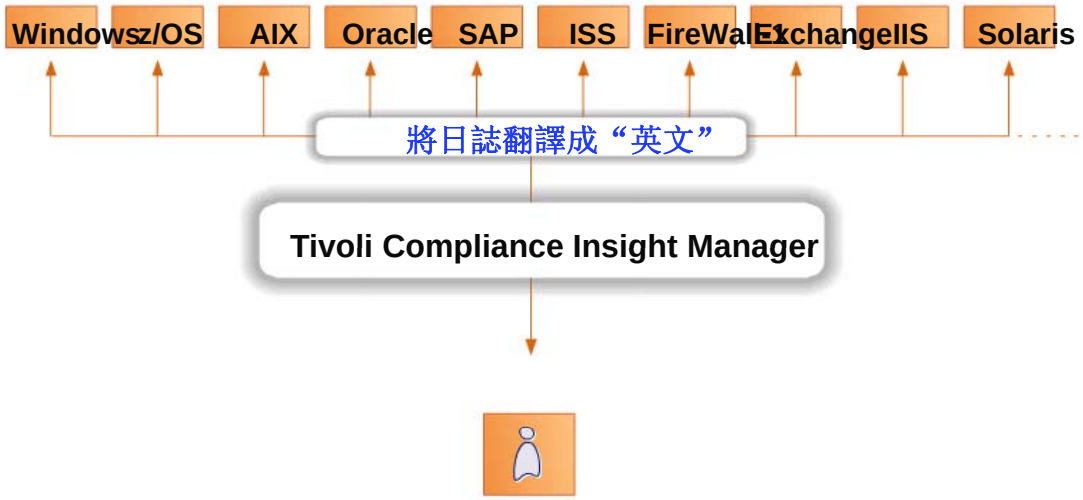
日誌連續性報告：
可即刻向稽核與審計機關證明您的日誌管理程式的完整性和持續性

如果沒有統一的日誌收集與分析，您會須要很多不同專業的顧問，而且花很多時間來執行健檢與稽核



Comprehend

通過自動翻譯實現日誌標準化



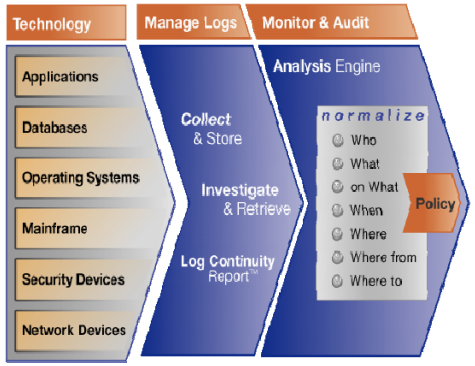
功能：

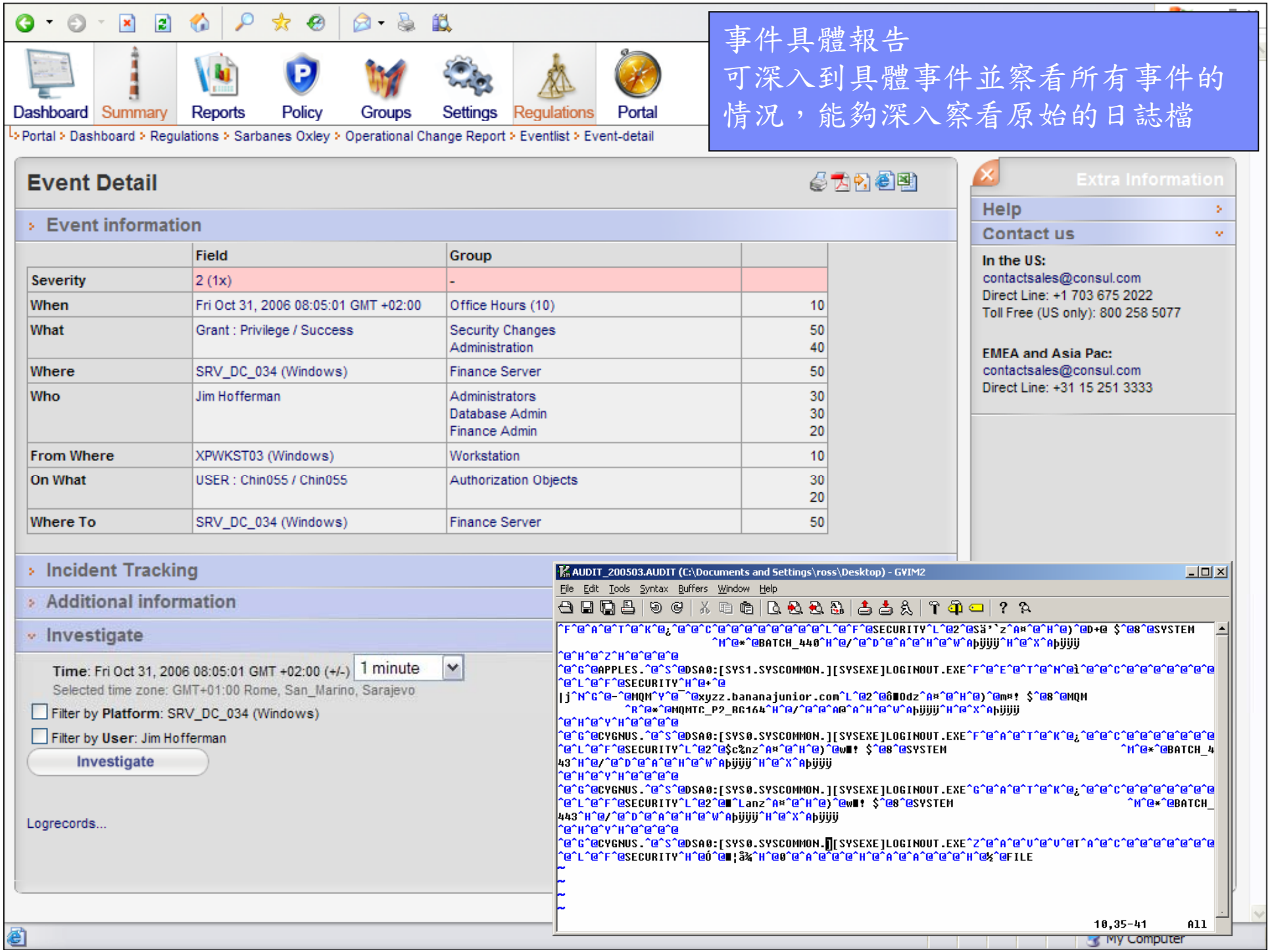
- 日誌的W7 標準化
- 將日誌專案與基準制度進行比較，從而判定違規行為，違規級別

成效：

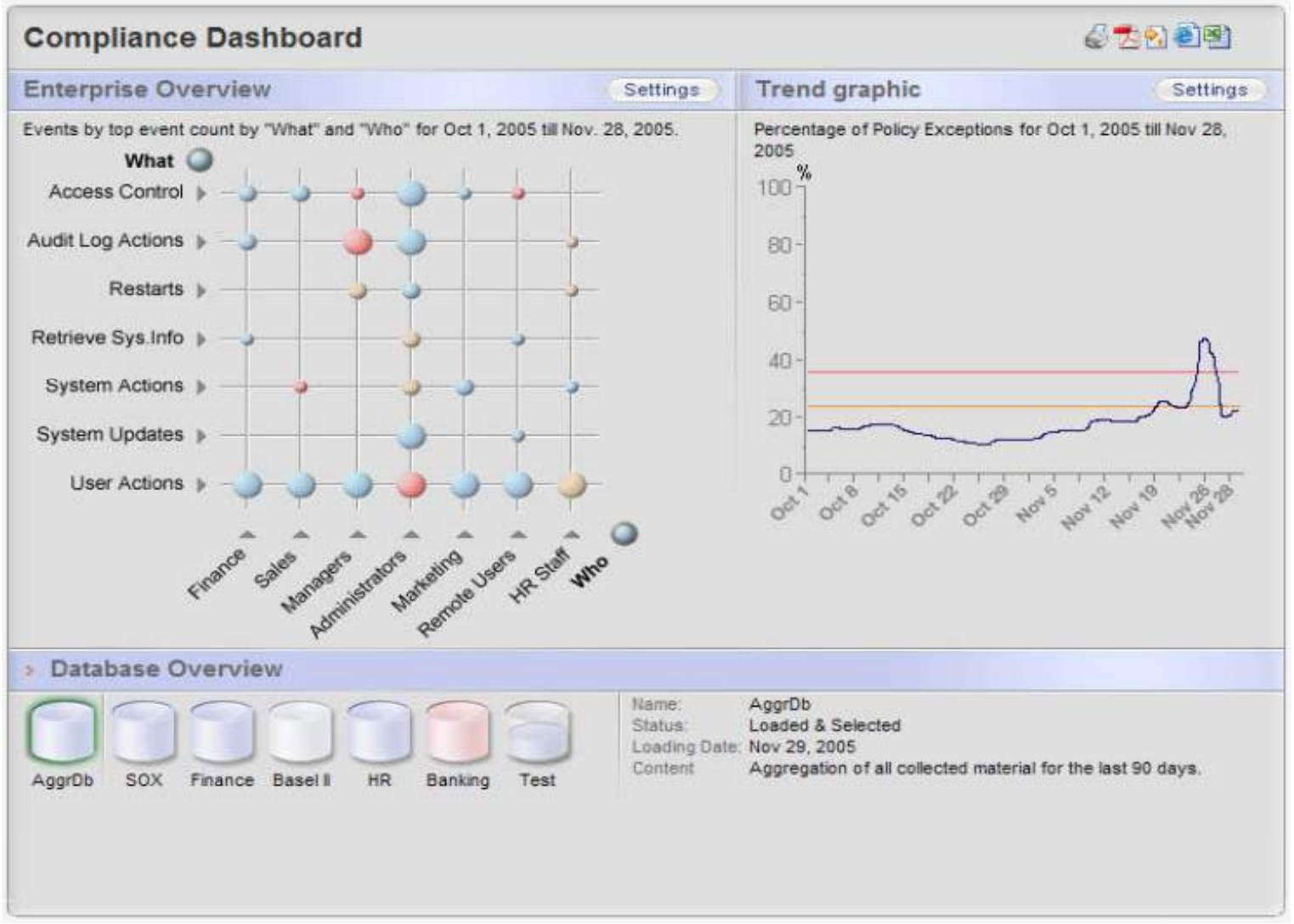
- 通過更少的資源和更低的成本來翻譯並監控所有的日誌
- 快速檢測並解決安全問題

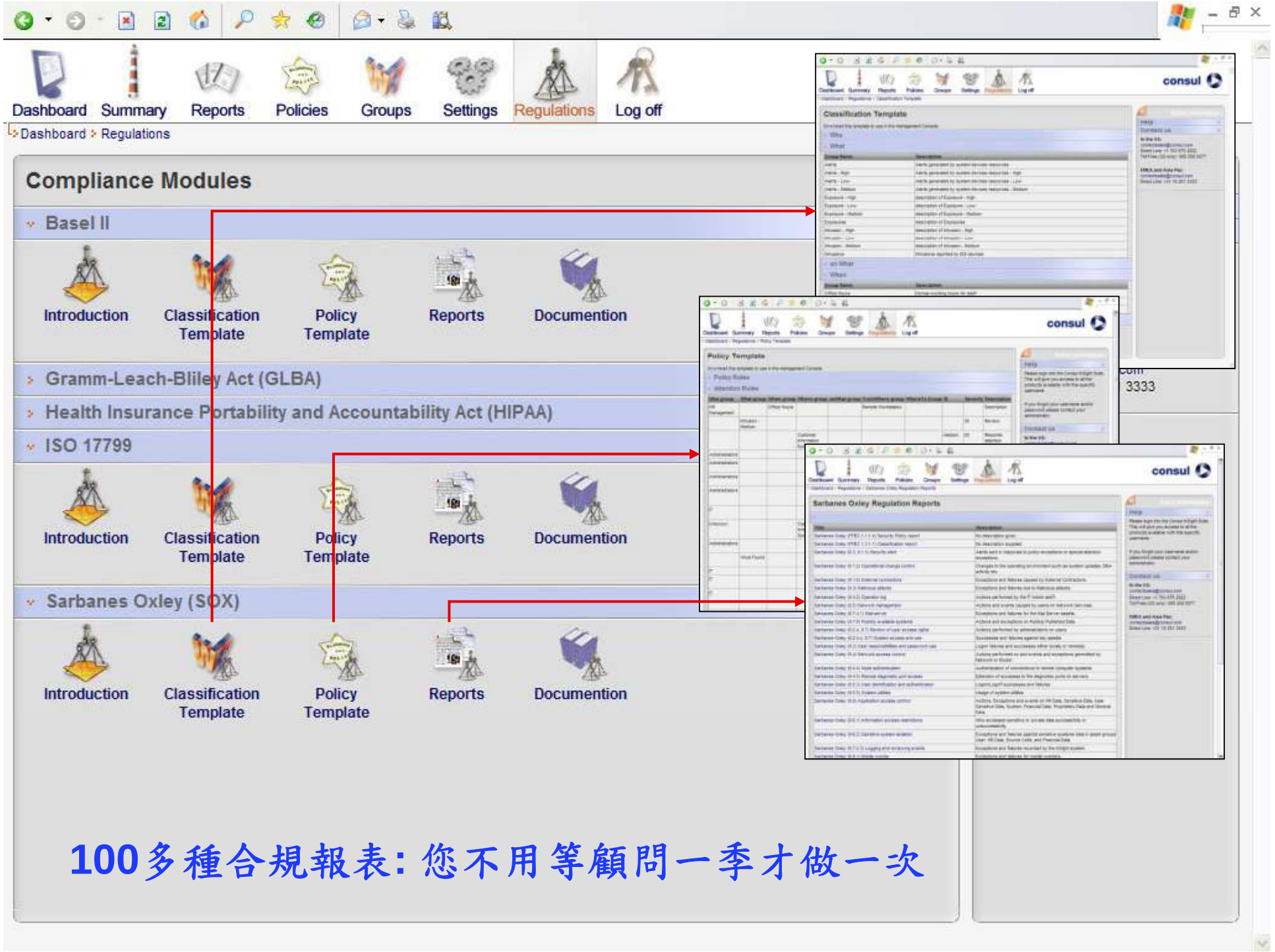
Who did What type of action on What?
When did he do it and Where, From Where and Where To?




事件具體報告
可深入到具體事件並察看所有事件的情況，能夠深入察看原始的日誌檔
Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-detail
Event Detail
Event information
Field
Group
Severity
2 (1x)
-
When
Fri Oct 31, 2006 08:05:01 GMT +02:00
Office Hours (10)
10
What
Grant : Privilege / Success
Security Changes
Administration
50
40
Where
SRV_DC_034 (Windows)
Finance Server
50
Who
Jim Hofferman
Administrators
Database Admin
Finance Admin
30
30
20
From Where
XPWKST03 (Windows)
Workstation
10
On What
USER : Chin055 / Chin055
Authorization Objects
30
20
Where To
SRV_DC_034 (Windows)
Finance Server
50
Extra Information
Help
Contact us
In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077
EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333
Incident Tracking
Additional information
Investigate
Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-)
1 minute
Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo
Filter by Platform: SRV_DC_034 (Windows)
Filter by User: Jim Hofferman
Investigate
Logrecords...
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
10,35-41 All
My Computer

合規儀表板: W7 處理的日誌 – 通過簡單的圖形匯總所有日誌檔，依照事件多寡與嚴重性來表示

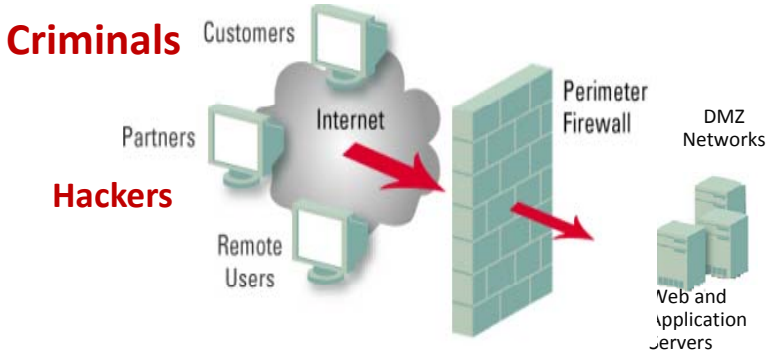


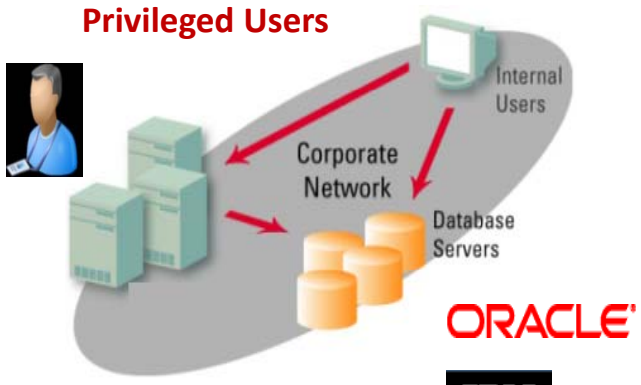


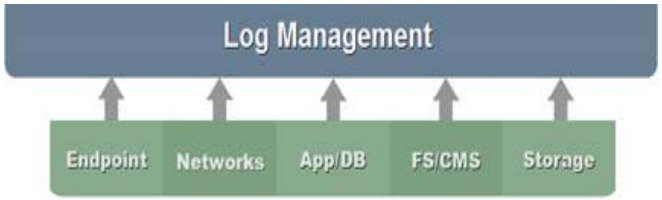
100多種合規報表: 您不用等顧問一季才做一次

但是有一些行為是系統日誌上沒有記載的，例如SQL指令的內容

- Complex environments
- Multiple access paths
- Firewalls, IDS/IPS can't prevent traffic that appears to be legitimate
- Most organizations have formal data security policies but ...
  - ✓No practical enforcement mechanisms
  - ✓No visibility into what's really going on -- especially with privileged users
- Dependent on native logs
  - Can't capture DBMS activity on their own
- SQL access is much "richer" than UNIX/Windows/Cisco logs
  - DDL (Create/Drop/Alter Tables)
  - DML (Insert/Update/Delete)
  - SELECTs (read operations)
  - DCL (Grant, Revoke)
  - SQL exceptions (SQL errors, etc.)



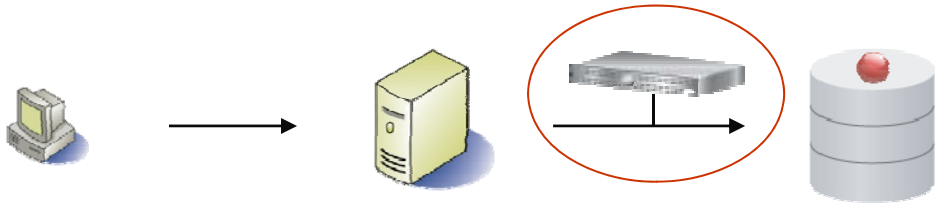




A Smarter Planet SmarterSecurity&Resilience

IBM的資料庫稽核與防護解決方案具備詳盡的稽核內容與安全項目

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



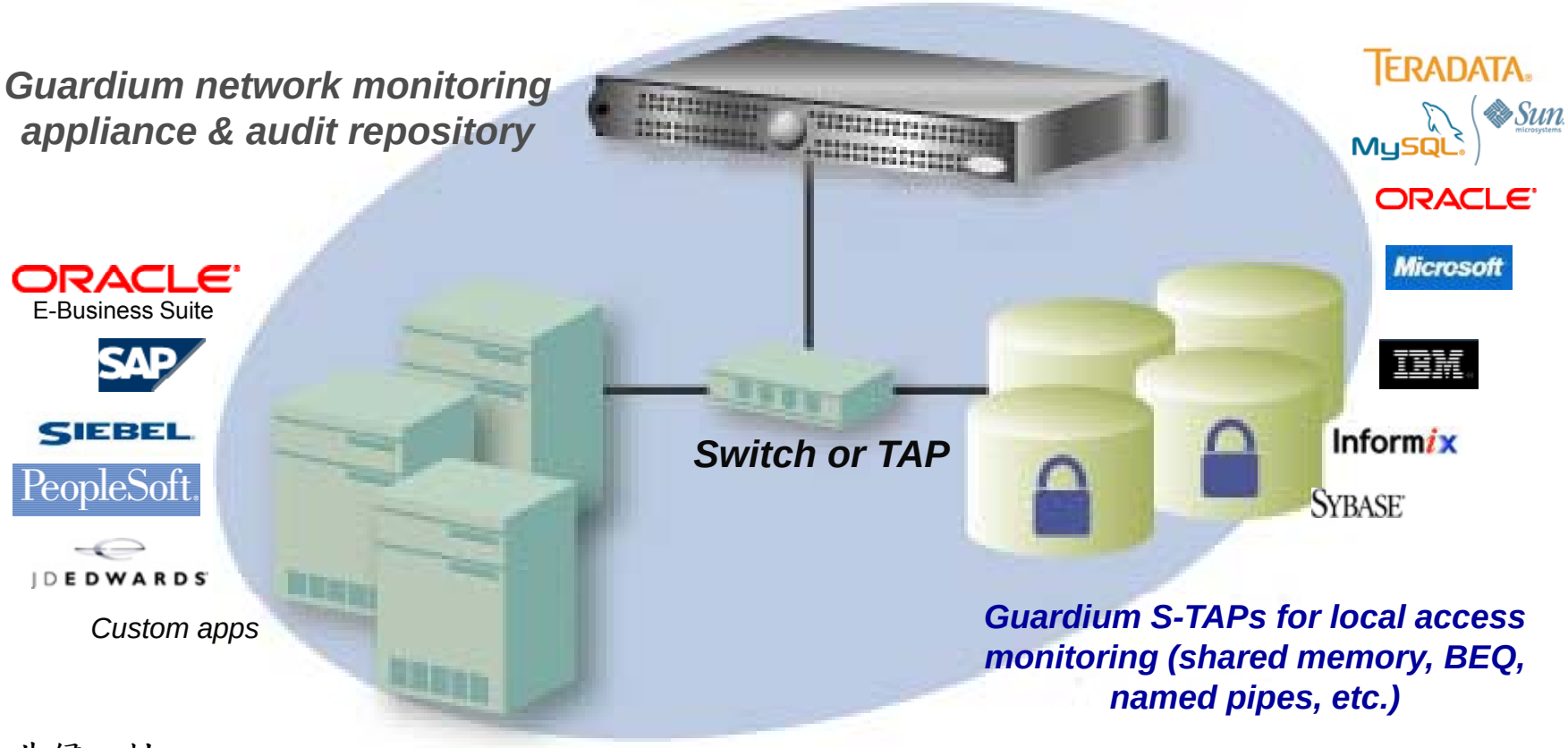
Client IP
Client host name
Domain login
Client OS
MAC
TTL
Origin
Failed logins

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

30

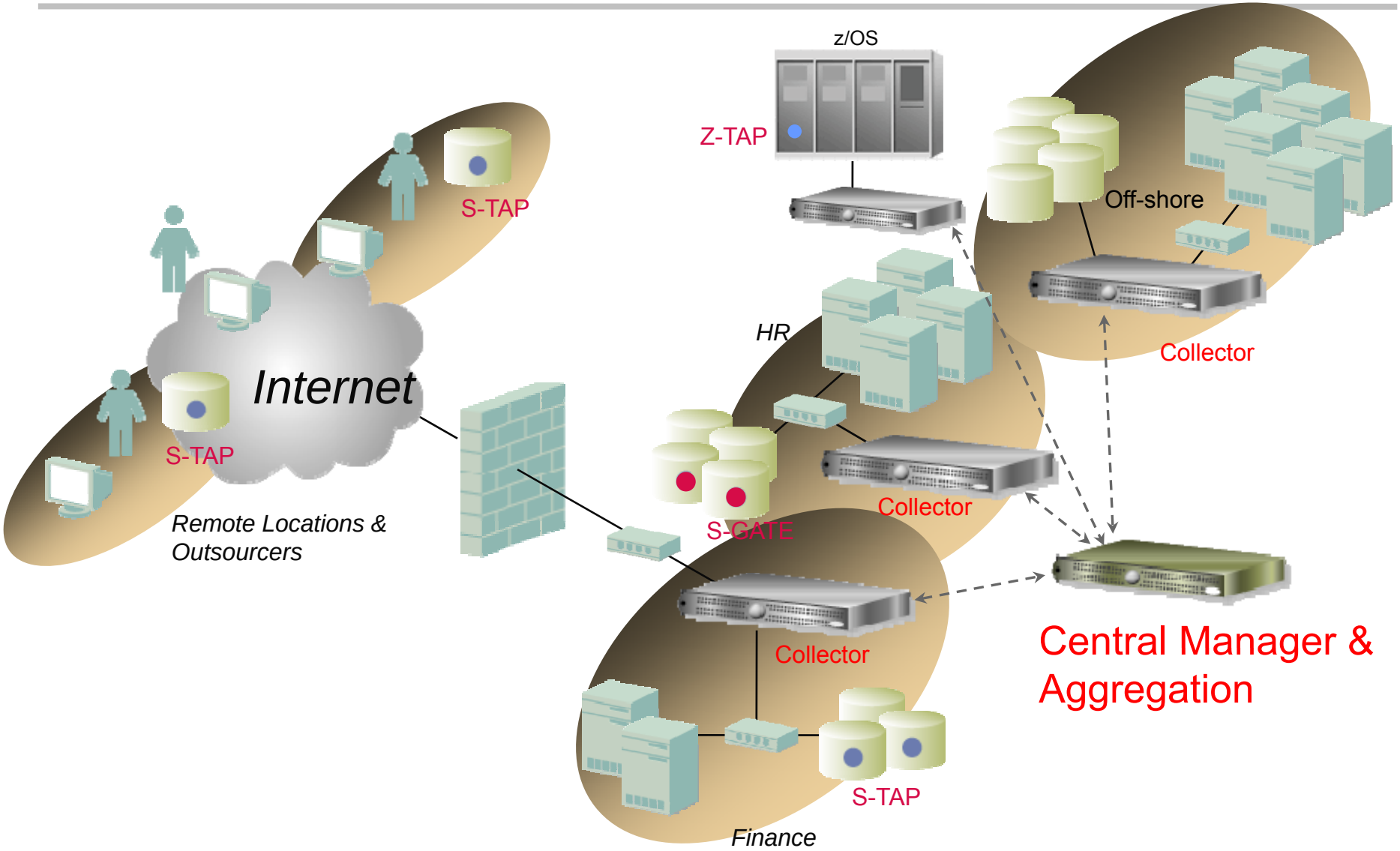
IBM的資料庫稽核與防護解決方案能在不影響資料庫系統的效能之下找出是哪個終端使用者用什麼方式存取資料庫的什麼內容

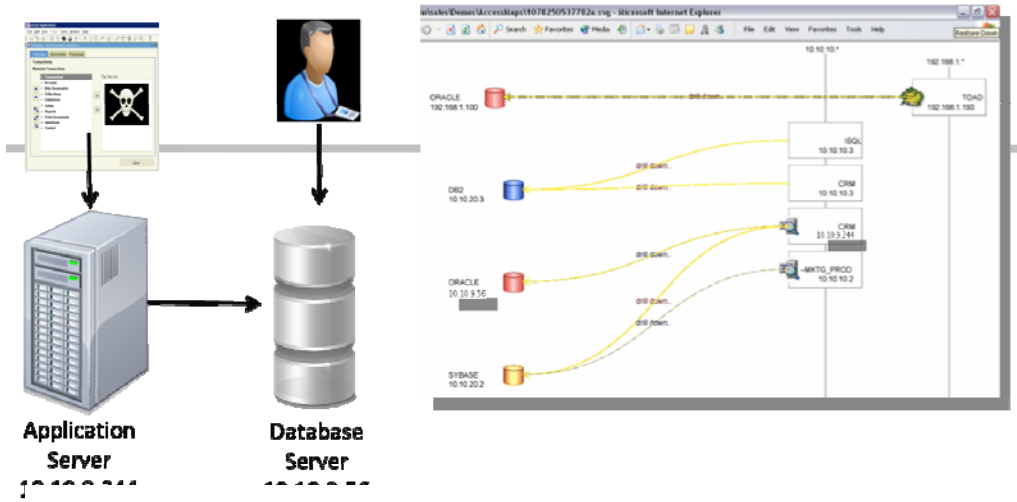


- 非侵入性
- DBMS獨立性
- 最小的系統影響
- 無需透過資料庫的日誌和稽核

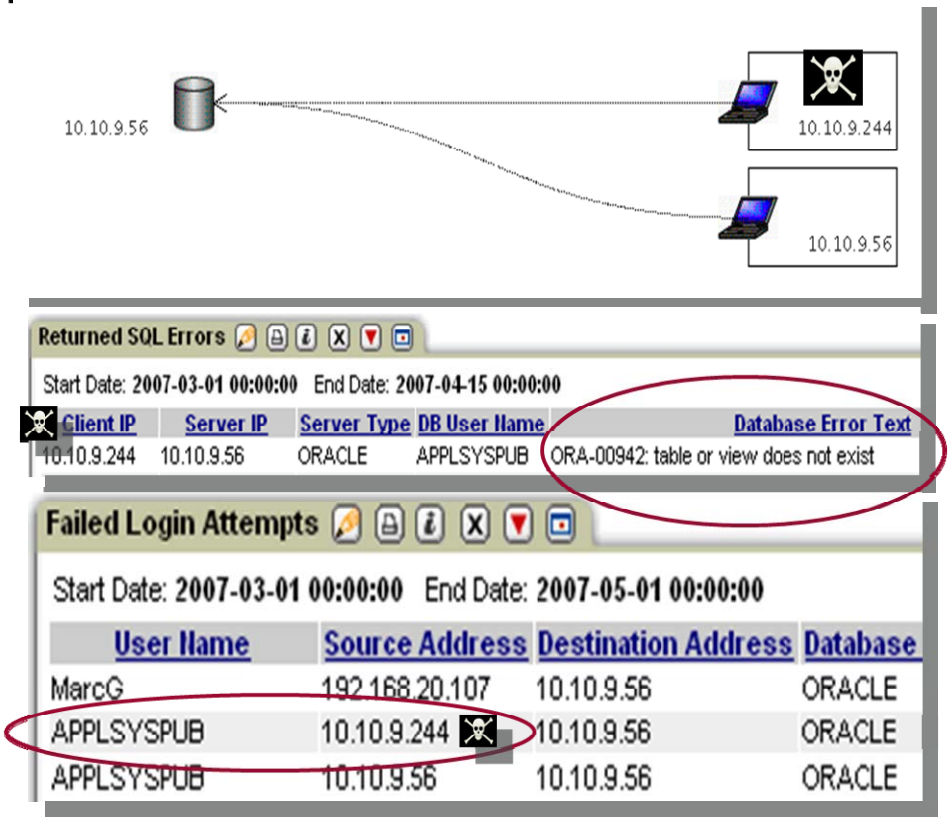
- 細緻精密的策略與監控
  - *Who, what, when, how*
- 即時警示
- 全面的活動監控包含本地端的存取

可擴展的多層次架構：除了完全不影響伺服器的網路監聽，也可以配上輕量級卻很有效的本機監聽語及時阻絕。並提供統一中控管理





透過本方案您可以了解有哪些應用系統會存取哪些資料庫，而除了應用系統的ID外有哪些人員的ID

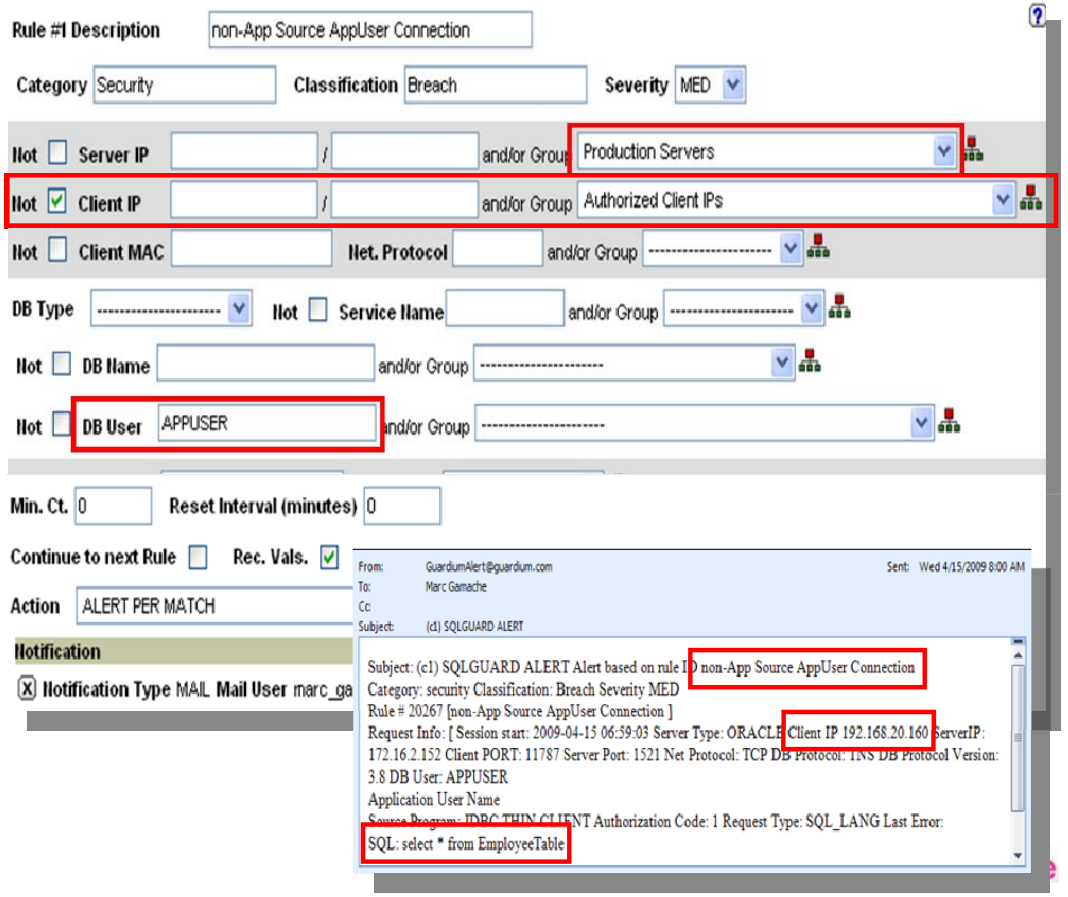


雖然是授權可以存取資料庫的應用系統ID ，但是為什麼是由非此伺服器所在的IP發出的呢？趕緊發出警示通知！

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

HARRY	select * from ar.creditcard where i<?	****************0002, ****************0003, ****************0004
JOE	select * from ar.creditcard where i<?	****************0001
JOE	select * from ar.creditcard where i<?	****************0002, ****************0003, ****************0004, ****************0005, ****************0006, ****************0007, ****************0008, ****************0009, ****************0010, ****************0011, ****************0012, ****************0013, ****************0014, ****************0015, ****************0016
JOE	select * from ar.creditcard where i<?	****************0017, ****************0018, ****************0019, ****************0020, ****************0021, ****************0022, ****************0023, ****************0024, ****************0025, ****************0026, ****************0027, ****************0028, ****************0029, ****************0030, ****************0031
JOE	select * from ar.creditcard where i<?	****************0032, ****************0033, ****************0034, ****************0035, ****************0036, ****************0037, ****************0038, ****************0039, ****************0040, ****************0041, ****************0042, ****************0043, ****************0044, ****************0045, ****************0046
JOE	select * from ar.creditcard where i<?	****************0047, ****************0048, ****************0049, ****************0050, ****************0051, ****************0052, ****************0053, ****************0054, ****************0055, ****************0056, ****************0057, ****************0058, ****************0059, ****************0060, ****************0061
JOE	select * from ar.creditcard where i<?	****************0062, ****************0063, ****************0064, ****************0065, ****************0066, ****************0067, ****************0068, ****************0069, ****************0070, ****************0071, ****************0072, ****************0073, ****************0074, ****************0075, ****************0076
JOE	select * from ar.creditcard where i<?	****************0077, ****************0078, ****************0079, ****************0080, ****************0081, ****************0082, ****************0083, ****************0084, ****************0085, ****************0086, ****************0087, ****************0088, ****************0089, ****************0090, ****************0091
JOE	select * from ar.creditcard where i<?	****************0092, ****************0093, ****************0094, ****************0095, ****************0096, ****************0097, ****************0098, ****************0099

為什麼有客服人員能在一分鐘內檢驗99個客戶的資料？
到底他在看什麼？



誰直接在資料庫伺服器上下DB指令？

```
login as: joe
joe@192.168.30.152's password:
Last login: Tue Apr 14 15:17:12 2009 from 192.168.20.160
[joe@u2 ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Apr 14 15:17:39 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> insert into AppUser.EmployeeTable values (1001,6,'Joe','Smith','Salary','Bonus',500000,1);

1 row created.

SQL>
```

How do you track users who 'switch' accounts (perhaps to cover their tracks)?

- Native DB auditing (& SIEM) tools can't capture original OS user information
- Other monitoring systems only provide OS shell account that was used

DB User Name	Sql
SYSTEM	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

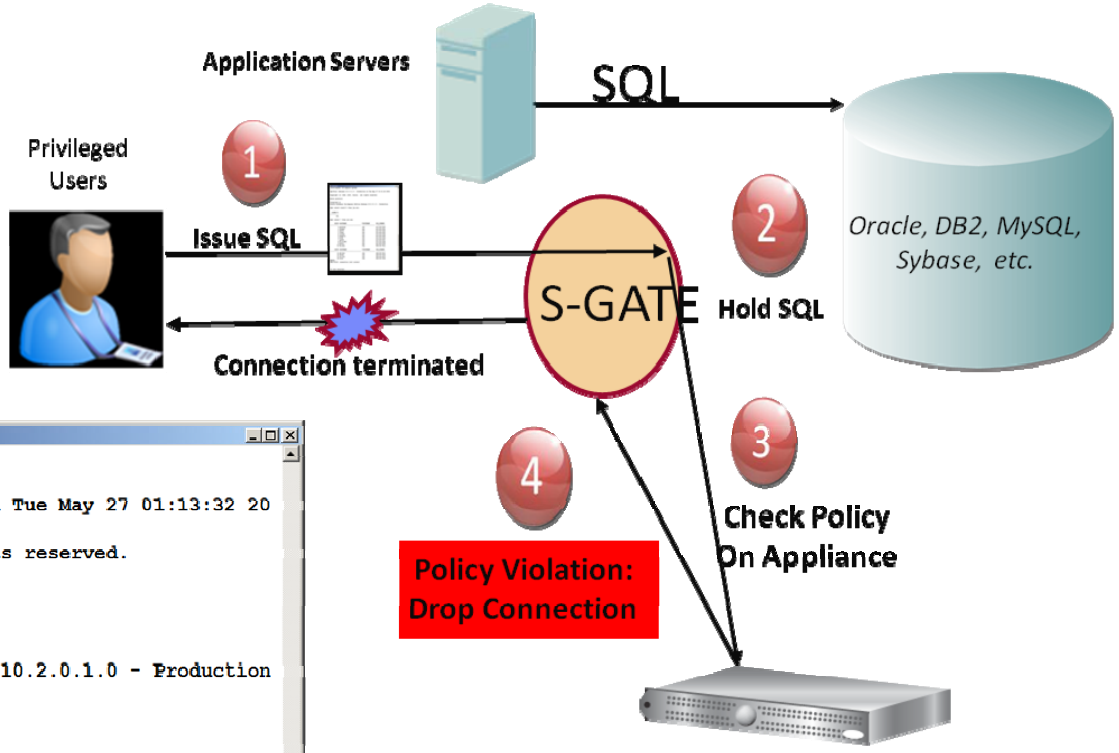
DB User Name	ShellAcct	Sql
SYSTEM	ORACLE	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

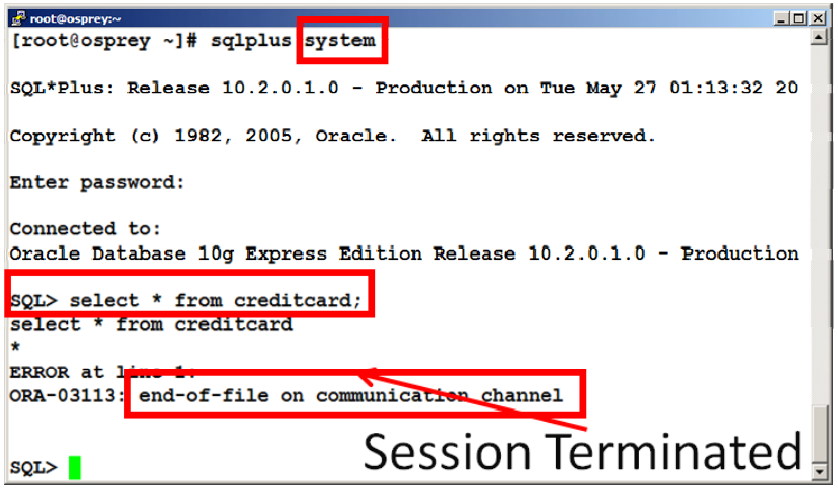
DB User Name	ShellAcct	OSUser	Sql
SYSTEM	ORACLE	joe	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

53

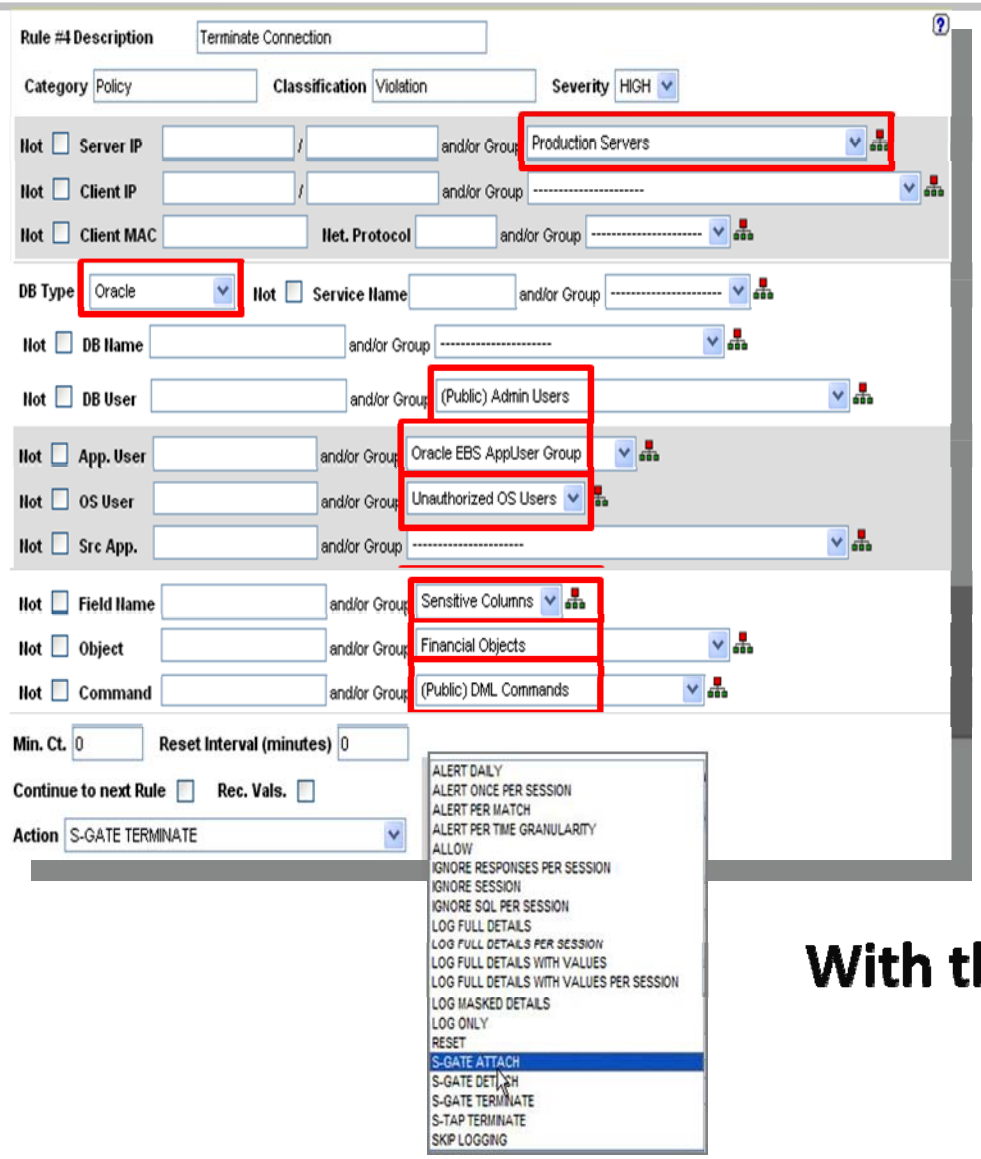
資料庫稽核與防護方案也能作及時阻斷

"DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database." Noel Yuhanna, Forrester, "Database Security: Market Overview," Feb. 2009.





本方案提供表列式親和性界面來定義及時阻斷的政策



Which Servers

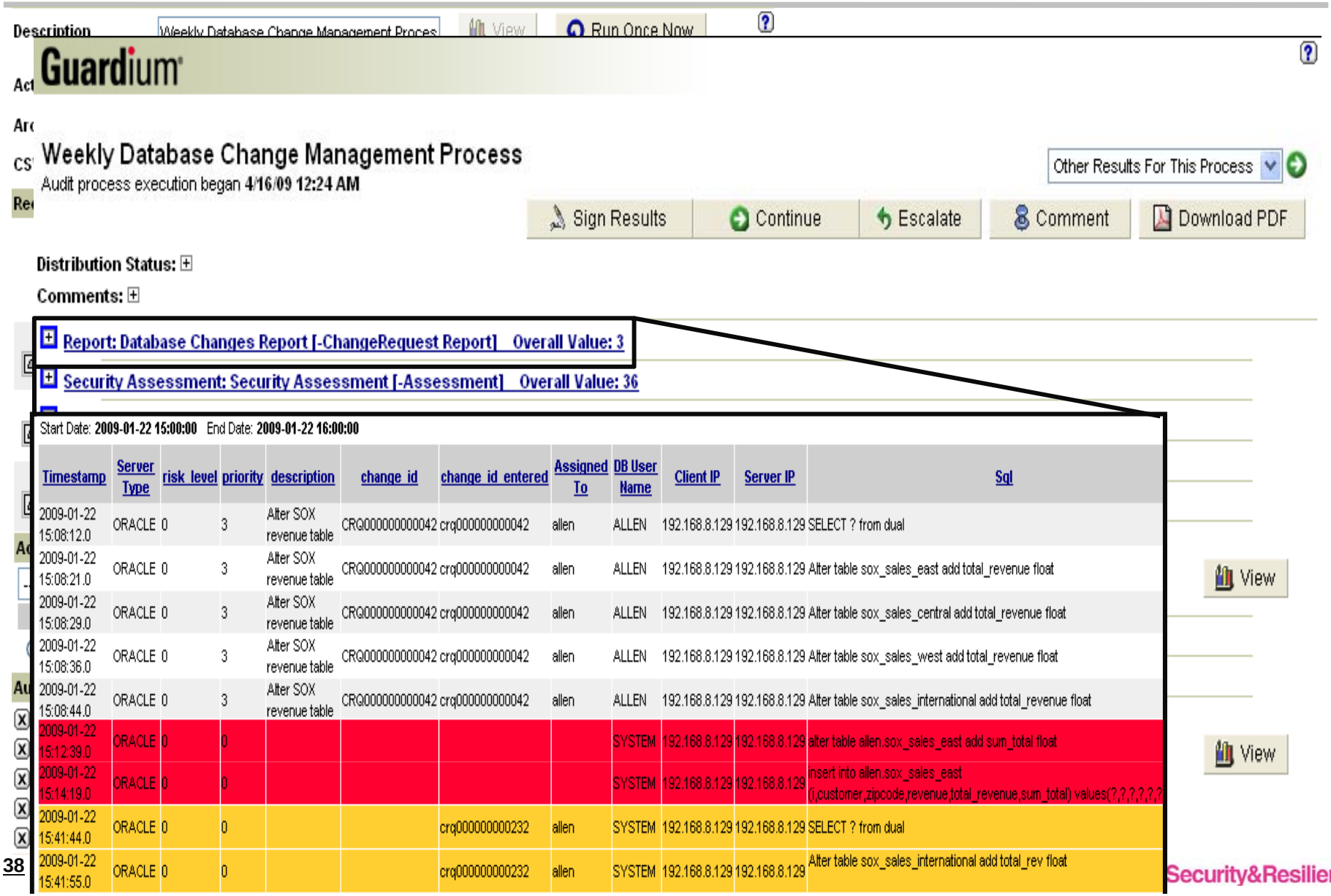
Which Databases

Which Users

Which Fields
Which Tables
Which SQL Commands

With the ability to terminate traffic!

資料庫稽核與防護方案可提供定期或不定期報表，可以概覽也可以追到詳細資料



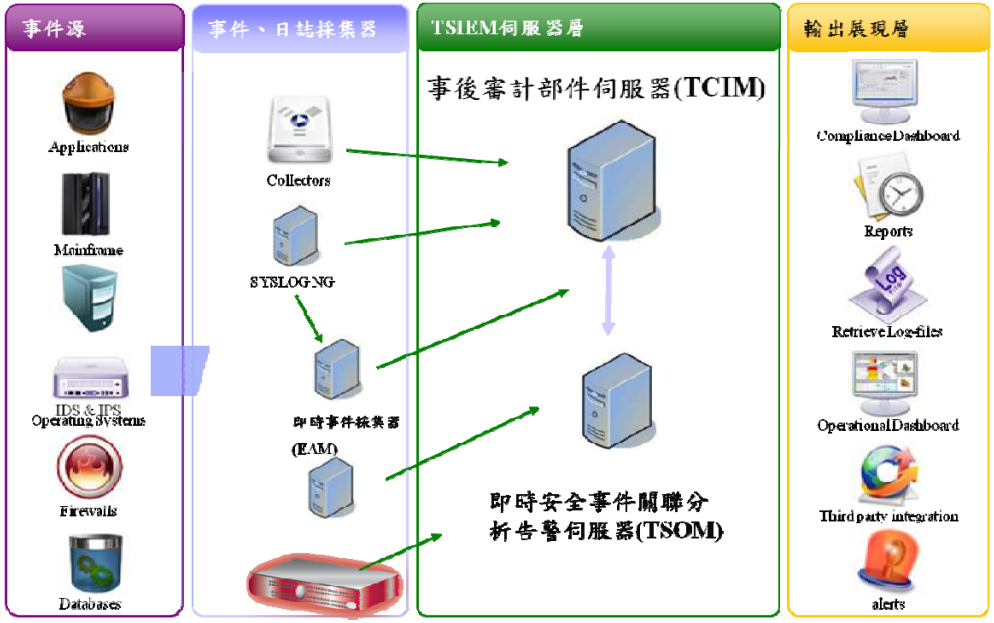
資料庫稽核與防護方案可以與日誌集中管理及分析方案整合，並提供只有它獨有的稽核資訊

Attacker Address	Target Address	Priority	Device Vendor	Attacker Port	Application Protocol	Destination User Name	Message
192.168.2.148	192.168.2.148	7	Guardium	20189	BEQUEATH	SYSTEM	select * from ar_trx_bal_summary

Policy Violations / Incident Management

Start Date: 2008-12-08 10:25:04 End Date: 2008-12-09 11:25:04

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary	HIGH



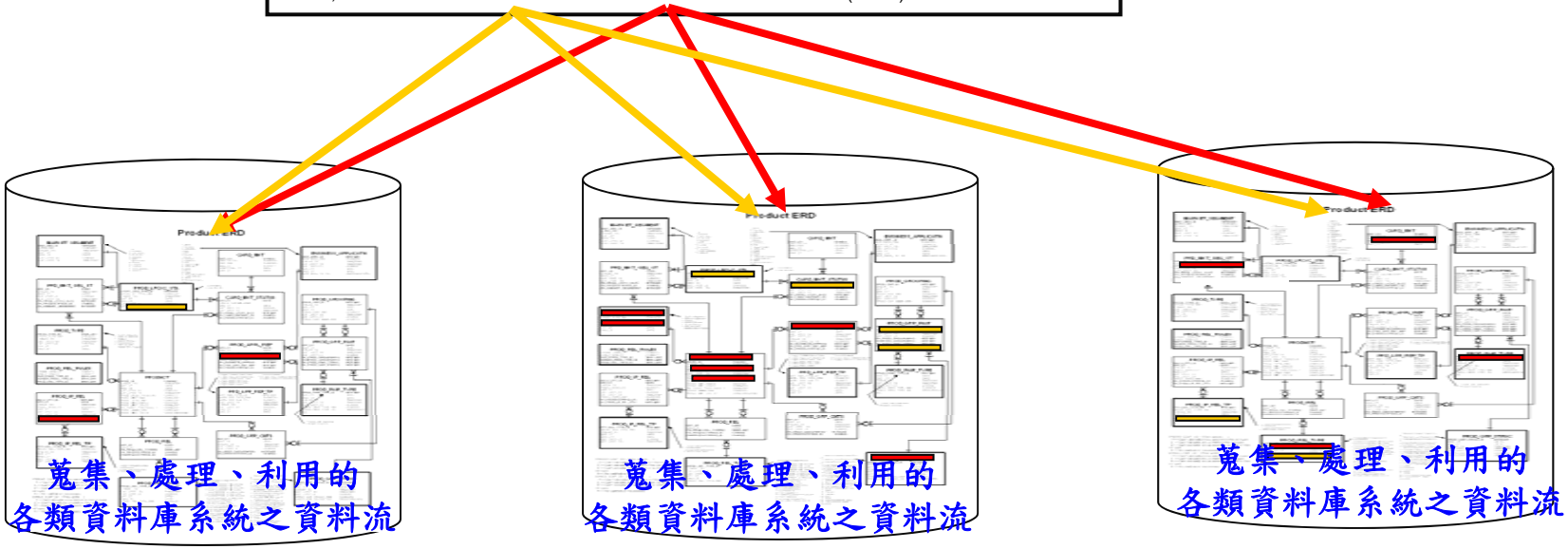
IBM測試資料保護方案對企業資料架構中隱私資料的控制點，提供一個簡單、可擴展、易於整合的隱私資料保護解決方案；打造出可信賴的架構環境，讓企業能以充分反映資訊價值及保障用戶隱私的方式，安心地把資訊資產用於業務最佳化。

But, Finding Sensitive Data is Hard

Sensitive Data Repository

Row	Member	SS #	Age	Phone	Sex
1	595846226	123-45-6789	15	(123) 456-7890	M
2	567472596	138-27-1604	8	(138) 271-6037	F
3	540450091	154-86-4196	22	(154) 864-1961	M
4	514714372	173-44-7900	55	(173) 447-8996	F
5	490204164	194-26-1648	4	(194) 261-6476	F
6	466861109	217-57-3046	66	(217) 573-0453	M
987,623	444629628	243-68-1812	25	(243) 681-8107	F
987,624	423456789	272-92-3629	87	(272) 923-6280	M

業務及交易流程之隱私資料運用



結合企業之業務推廣、資訊交互運的業務及交易流程，針對蒐集、處理、利用的各類資料庫系統之資料流進行隱私資料控管

隱私資料保護 - 提供了自動化的資料轉換、變形能力，能夠輕鬆地跨越多個資料庫將企業中涉及的各種個人資訊或保密資訊實施脫密、漂白處理。不但幫助企業實現法規遵，還能夠為測試或應用外包等提供無損企業利益的脫密資料版本，實現企業隱私資料的有效保護

Lookup 陳筱玲→陳雲林

Aging 加三天

Semantic 可驗證的假身份證字號

Hash Lookup 地址甲→Hash→地址乙

Random 亂數生成序號

隱私資料保護 - IBM Optim 針對不同資料格式提供不同遮蔽機制，能夠輕鬆地執行身份刪除(De-Identification), 去個人化(Depersonalize), 匿名化(Anonymize)及身份遮蔽(Masking)並同時保持資料完整性

Intelligent Data Masking

A comprehensive set of data masking techniques to transform or de-identify data:

- String literal values
- Character substrings
- Random or sequential numbers
- Arithmetic expressions
- Concatenated expressions
- Date aging
- Lookup values
- Intelligence

Example 1

Customer Information

Customer No.	123456	PID	E165851537
Name	李大雄		
Address	四維三路2號		
City	高雄市	Zip	80203

Data is masked with contextually correct data to preserve integrity of test data

Example 2

Personal Info Table

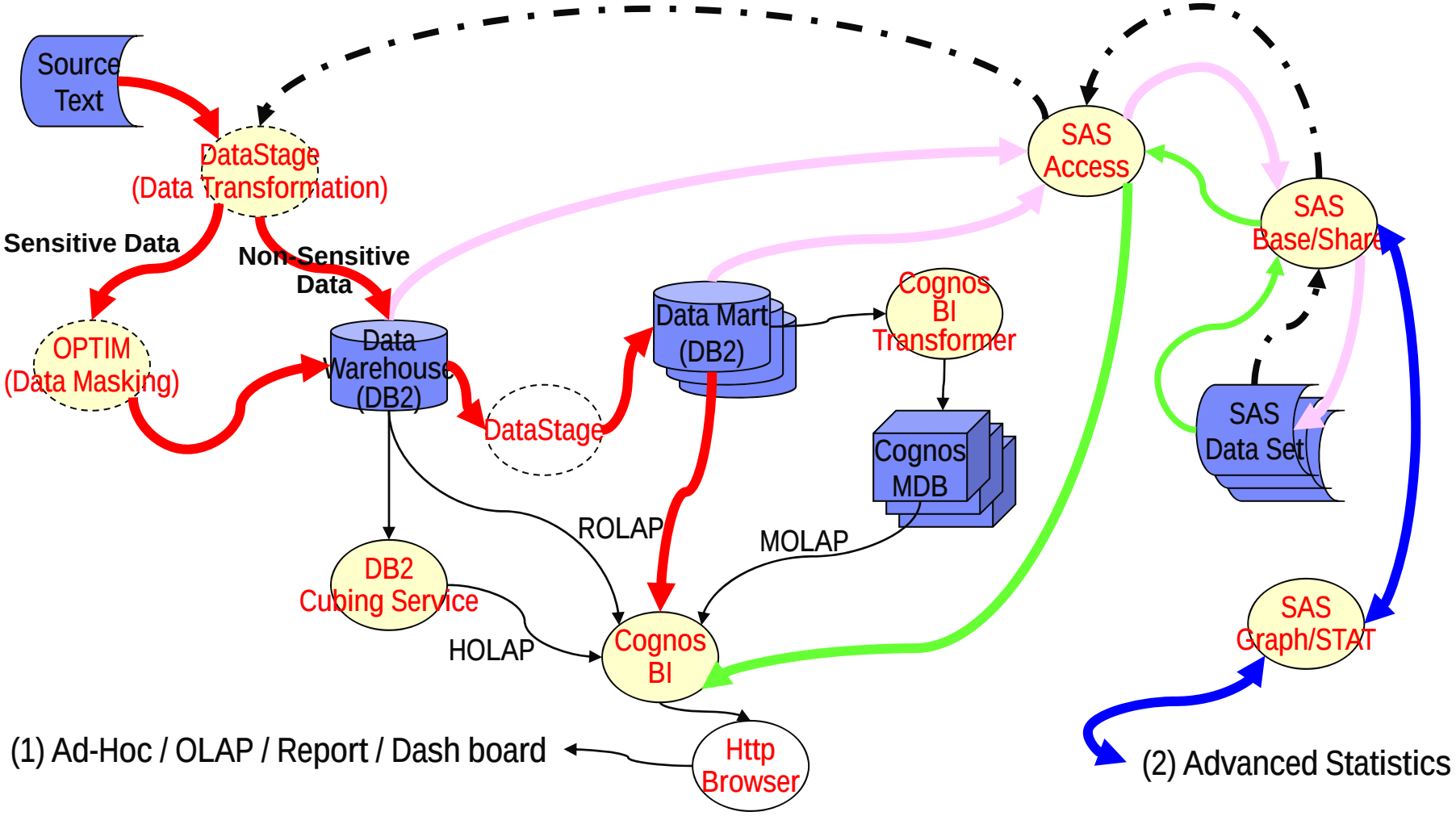
Account	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	Pablo	Picasso

Referential integrity is maintained with key propagation

Event Table

Account	FstNEvtOwn	LstNEvtOwn
10002	Pablo	Picasso
10002	Pablo	Picasso

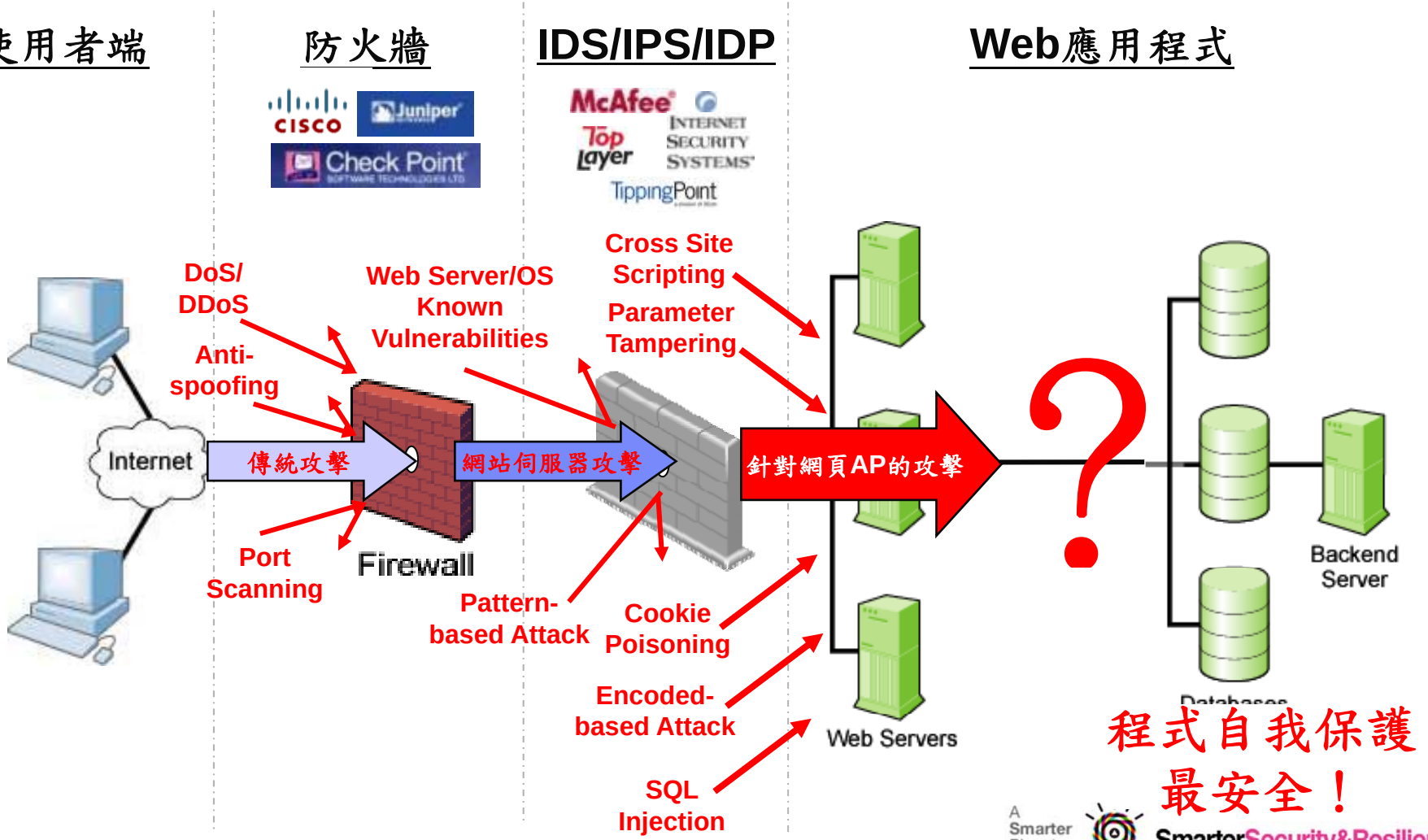
隱私資料保護 - 參考使用案例之架構



除了以上能力以外，IBM Optim還為大多數主流套裝應用—如:SAP，Siebel，Oracle ERP等提供了定制能力，同時能夠支援幾乎所有主流伺服器、作業系統與資料庫產品，並提供多平臺的集成訪問能力。—— 除了IBM Optim，目前還沒有任何其他產品能夠提供如此豐富的軟硬體平臺與套裝產品支援！

2008年，一種名為SEO程式碼植入（injection）或毒害（poisoning）的新型態資安威脅，影響全球高達120萬個網站，其中不乏一些相當知名者。隨著災情逐漸緩和，全世界開始慢慢體會到應用程式已成為駭客攻擊的首要目標。

從Web應用程式運作架構，看各類攻擊對網路節點的防禦能力



A Smarter Planet SmarterSecurity&Resilience

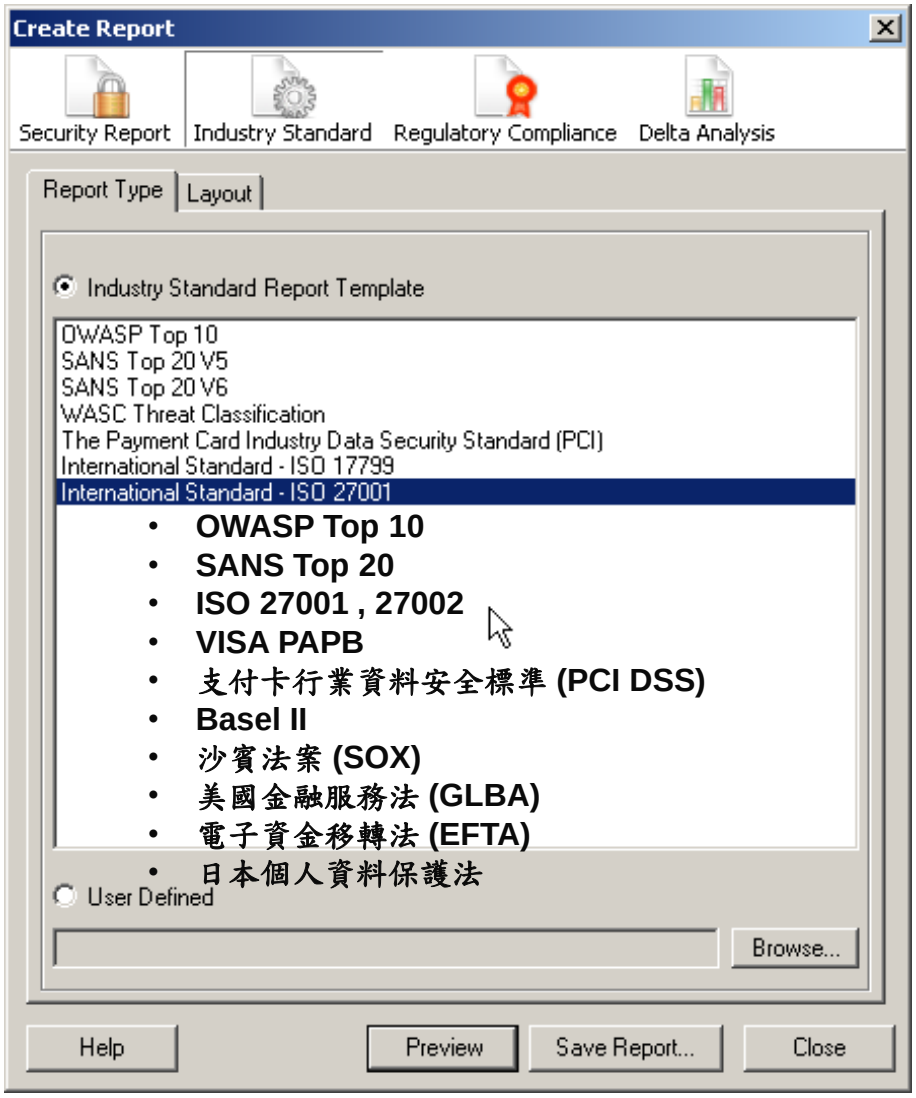
應用程式最危險的地方，或許在於設計人員無法在程式部署完成以前全面掌握其組成成分與安全性，等到程式建置完成後，各種惡意程式與安全弱點可能早已嵌入應用內，任何改變也為時已晚。

案例: Parameter Tampering
可直接讀取其他人的交易內容-授權機制有嚴重漏洞

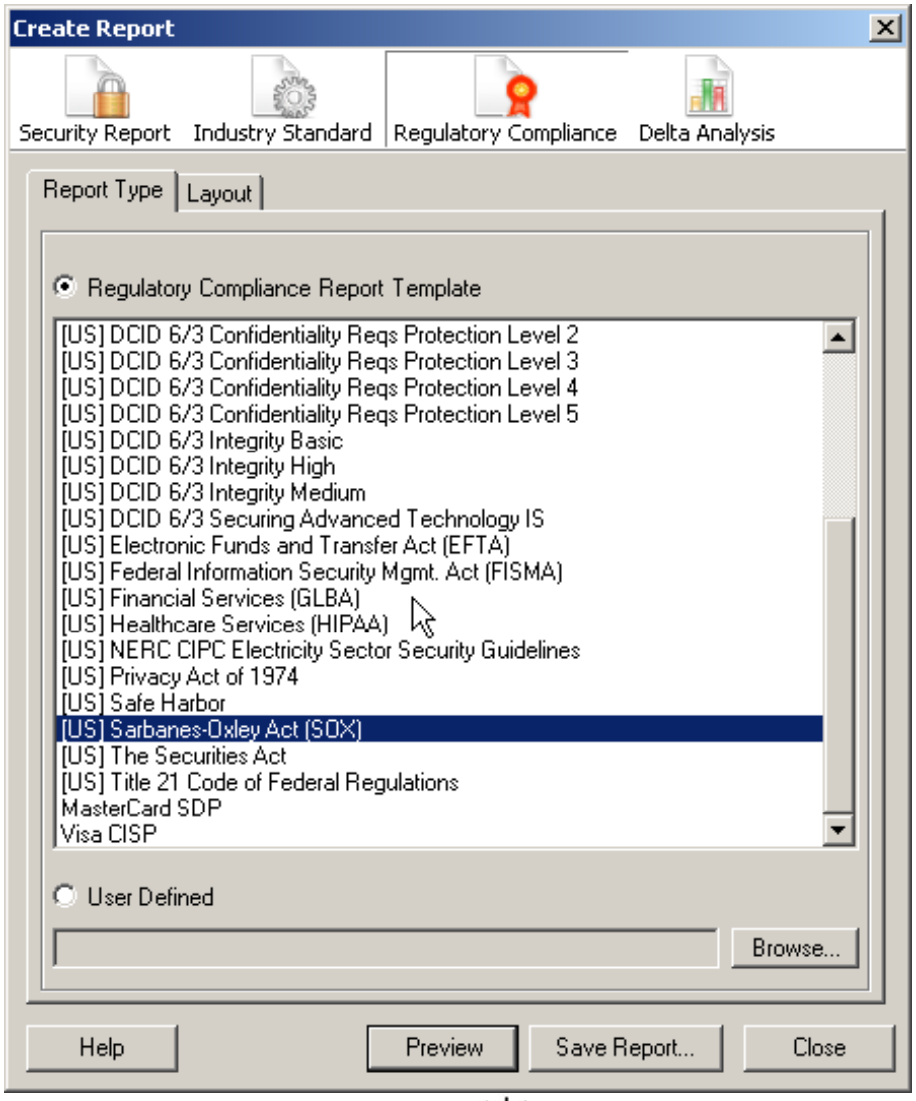
- 在網址列把reserID改為2001200
  - 成功顯示出其他客戶的交易明細包含正確的E-mail

案例: SQL Injection 盜取帳戶資料

IBM網頁應用程式保護機制與開發規範方案內建近50種產業標準、資安法規的報告範本，並將之融入企業應用安全整體分析之中。



- **OWASP Top 10**
- **SANS Top 20**
- **ISO 27001 , 27002**
- **VISA PAPB**
- **支付卡行業資料安全標準 (PCI DSS)**
- **Basel II**
- **沙賓法案 (SOX)**
- **美國金融服務法 (GLBA)**
- **電子資金移轉法 (EFTA)**
- **日本個人資料保護法**

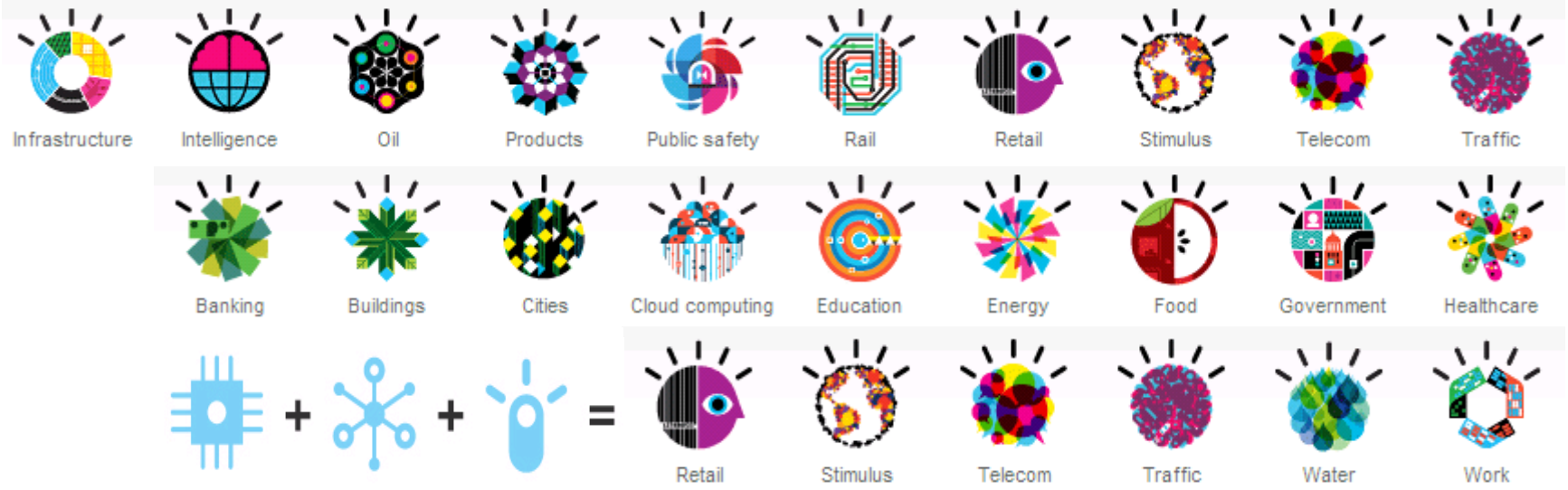


因應『新版個資法』的 法規要求及對IT系統影響；IBM從資料處理流程的控管角度 ，針對所涉及三大IT議題，提出因應方針及相關流程整合 解決方案。完整包含顧問服務、軟硬體系統

法規要求	IBM解決方案套餐	IBM 解決方案	產品與服務對應
個資法	風險與弱點評估 制訂資安及隱私政策	■ 個資文件與資料分類分析與保護政策的訂定 ■ 制定個人資料保護政策並進行隱私資料流分析	■ GTS consultant ■ GTS consultant
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	資料運用與保護	■ 入侵防禦弱點評估諮詢與設計服務 ■ 隱私與測試資料保護弱點評估諮詢與設計服務 ■ 網頁應用程式保護機制與開發規範暨安全性檢測服務 ■ 主動式入侵防禦及弱點保護系統規劃與建置服務 ➢ XML/ WS 防火牆規劃與建置服務	■GTS + Tivoli ISS Enterprise Scanner ■GTS + **IM Optim** ■GTS + **Rational AppScan** ■GTS + Tivoli ISS IDS/IPS ■GTS + WebSphere DataPower
	節點資料洩漏保管	■ 端點設備資料外洩預防規劃與建置服務 ■ 資料加密規劃與建置服務 ■ 磁帶端點設備機加密與保管解決方案 ■ 雲端桌面資料保護解決方案	■GTS service (Digital Guardian) ■GTS service ■STG tape drive, library ■GTS service (desk top cloud)
資料外洩損害賠償， 非公務機構需證明「無故意或過失責任」，才能免責	資料外洩分析與處理	■ 內部使用者行為稽核規劃與建置服務 ■ 資料庫稽核與防護系統規劃與建置服務 ■ 日誌集中管理及分析系統規劃與建置服務 ■ 身分辨認與授權管理規劃與建置服務	■GTS service (Intellinx) ■GTS + **IM Guardium** ■GTS + **Tivoli SIEM** ■GTS + Tivoli Identity Mgmt, Access Mgmt

Q & A

The technology is here.
The people are ready.
The time is now.

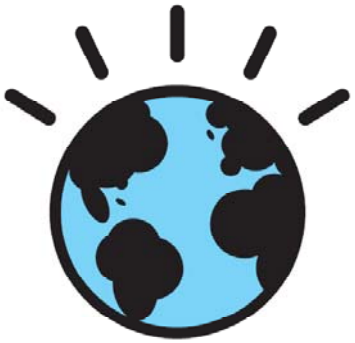


IBM Global Services
3-4F, No.7, Song Ren Road,
Taipei, Taiwan

Produced in Taiwan

Julian Lin
0932-035660
julin@tw.ibm.com

附件



ISS：網路入侵防護解決方案

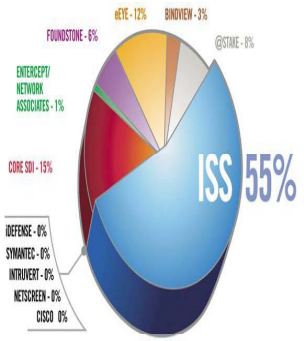
企業挑戰

當個資法通過後，如確保個資外洩問題？確認你的網路應用系統安全度?

- Web 網站使用了防火牆，所以很安全?
  - Web 網站提供對外服務，防火牆必須允許其通訊協定，但對於善意及惡意使用者並無法識別
- Web 網站使用IDS，所以很安全?
  - IDS 針對網路層之惡意行為進行過濾，對於以合法掩護非法之正常連結行為無法識別
- Web 網站使用了 SSL 加密，所以很安全?
  - SSL 對於網站發送及接收之資訊都進行加密處理，但對於儲存於網站後端資料庫之機密資料並無法保障其機密性

誰最瞭解網際網路的風險 ？– IBM ISS X-Force 團隊

1. 長達14年的研發歷史
2. 專注于發現和分析安全風險，開發技術對策
3. 每半年發佈一次網路整體風險趨勢狀態報告
4. 每年發佈30 次以上的安全建議和警告
5. 每月找出200 多個新的攻擊手法
6. 維護超過 36,000 個漏洞的安全資料庫
7. 開發了 6000 多個檢查項用於檢測和發現攻擊手法
8. 發佈X-Force月度威脅觀察報告 (XFTIM)
9. 2008年，研究與發現7406個安全漏洞
10. CVE組織創始人之一，相容 CVE/CPE/CVSS



高風險漏洞發現比例

Frost & Sullivan 2006 , Internet

入侵防禦系統 Proventia® GX 價值主張

1. 全世界 IPS/IDS 市佔率 No.1 (包含台灣)
2. 有效偵測已知、未知攻擊行為，發現攻擊立即阻擋
3. 偵測 3,000+ 入侵攻擊
4. 支援「 X-Force 虛擬補丁(Virtual Patch)」，使用者不必馬上更新系統的 Patch，即可在攻擊發生前完成防禦措施
5. 「虛擬 IPS」功能：依客戶環境同時支援超過「1,500」組以上監控防護政策
6. 高彈性佈署：線上模式、模擬模式、與監控模式。
7. 支援 HA 與 By Pass 模組，保障客戶「服務」不中斷

成功案例 References

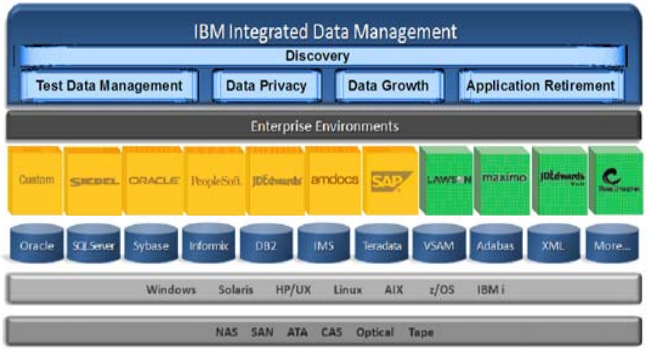
1. 中鋼：入侵防護系統的部署有效阻擋了來源於外部的攻擊行為，也即時檢測出對於內部伺服器訪問的資料報文中是否存在可疑行為，並及時告警。
2. Grand Hyatt：簡化連鎖飯店的資安管理, 及降低資安設備的投資,多合一的資安設備整合防火牆, 入侵偵測系統, 防毒, 網站存取過濾等功能, 有效防範日新月異的安全威脅。
3. 更多其他案例如：TSMC、UMC、Army、CHT、Sparq、CSIST、BOL、CA、SCB、Taishin Bank、TCB、DOH

型號	偵測埠	效能 / 保證頻寬	優惠售價（未稅）
GX3002	2	10Mbps	NT$ 288,000（含第一年維護）
GX4004-V2	4	800Mbps	NT$ 968,000（含第一年維護）
GX5008-V2	8	1.5Gbps	NT$1,968,000（含第一年維護）

IBM Optim：測試資料保護

Production System

- 提升生產力 *Improve Productivity*
- 提升系統效能 *Improve Systems Performance*
- 降低成本 *Reduce Costs*



Optim Data Archiving

- 提升服務水準(SLA)並降低風險
- 控制成本(硬體空間、軟體License、人力成本)
- 簡化 IT 基礎架構
- 實作符合成本效益的階層式儲存策略
- 滿足資訊控管需求
- 掌控快速增加的資料
- 透過資料生命週期管理(封存、儲存、存取、刪除)企業資料 (Data Life Cycle Management)
- 進行業務永續方案
- 增加企業應用程式的商業價值
- Garner report 調查現有客戶和潛在客戶，大家一致推崇和信賴 的產品

Non-Production System

- 縮短測試時間 *Shorten Time-to-Market Schedule*
- 遮蔽機密資料 *Mask confidential data*
- 符合保密規範 *Comply with privacy policies*

Optim Data Privacy

- 遵循個資法，保護機密客戶資訊
- 避免罰款和處罰。避免負面宣傳（損害品牌形象，失去市場占有和收入損失）
- 符合特定行業和全球資料隱私的立法
- 保護公司（品牌資產/法律行動）
- 保護客戶（個人資料隱私/資料破壞）
- 使用各種已驗證過的資料遮蔽技術去遮蔽機密資料
- 使用有效的遮蔽數值來取代機密資料
- 保存遮蔽資料的完整性，使用於測試，培訓和系統開發的環境

Optim Test Data Management

- 減少線上作業系統停機時間與不可靠的應用性能
- 降低在正式作業環境中發現應用系統缺陷的成本
- 加速部署新的應用系統功能，及時支持客戶服務和業務計劃
- 在激烈競爭的商場，更快地提供產品和服務
- 建立符合實際、適當大小的測試資料庫，小到足以確保加快測試運行，但是又內含足以因應系統測試所需的完整資料
- 以快速便利的方式建立系統測試必需的臨界點資料，協助找出應用系統程式的缺點和不完善的邏輯
- 比較系統單元測試前，後資料的異動情況，新增、修改、刪除的差異結果，可以用不同顏色顯現於結果報表中，協助系統開發人員快速地驗證系統功能

AppScan：Web 應用程式零漏洞方案

企業挑戰

當個資法通過後，如何因應法規變化? 要確保企業商譽與客戶關係，您準備好了嗎?

- 75%以上的駭客都針對網路應用系統攻擊，目前已經在運行的網站到底是不是安全的？
- 委外開發的Web應用系統，如何驗收確認其安全無虞?
- 網站應用系統愈搞愈大，功能愈來愈多，程式愈寫愈複雜，安全性怎麼兼顧？公司內部缺乏具備網站應用系統安全know-how的專業人員，就算你告訴我有漏洞，我們的人一時之間也不會改…除了委外處理別無他途了嗎？
- 網站才剛剛經過委外的資安專家檢測，目前沒有重大的漏洞，但駭客不斷研究新的攻擊手法，等到下次檢測還要好幾個月，這段時間不會有事嗎？

核心價值-產品功能

IBM Rational AppScan為Web應用程式安全性檢測軟體的先驅，市佔率世界第一。Gartner 的研究預測至 2010 年，將有 80%的企業會遇到應用程式安全問題。AppScan於整個軟體開發的生命週期中皆可應用，簡介如下：

- 是一套自動化弱點掃描工具，用來檢測Web應用系統的安全性，找出系統的資安漏洞，並一一提供詳盡的處理建議。
- 可簡化發現與修復Web應用系統安全性問題的工作，降低維護資訊安全的成本。
- 黑箱測試：模擬各種駭客攻擊的手法，以無害的方式去使用運行中的Web應用系統，判斷系統是否存在各種安全性問題，並按照問題輕重緩急順序，提供可立即處理問題的建議做法。
- 白箱測試：分析提供的原始碼，判斷系統是否存在各種安全性問題，指出有安全問題的原始碼位置，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法。

與競爭者 的比較：市面上唯一整合黑箱與白箱的工具

1. HP WebInspect：無法提供符合國際認證標準的報表，在台灣無法提供即時的支援。
2. Fortify：其solution主要在於原始碼的靜態安全性分析檢測，支援檢測的開發語言類型眾多，但缺乏黑箱測試的解決方案，僅分析原始碼，會遺漏一些系統整合運行時才檢測得出的弱點，使用上也較侷限於開發人員。AppScan目前除黑箱測試的解決方案外，已有白箱測試解決方案，才是完整的安全性檢測管理方案。如果客戶都是委外開發暫大多數，其實不需要幫委外廠商購買白箱測試的軟體去測他們的程式碼，應該是購買黑箱測試的產品，確認程式沒有安全性的漏洞，才讓他們上線。
3. Dragonsoft， FoundStone等其他產品：OS/Network方面的弱點評估軟體，非網頁應用程式安全性檢測的產品。客戶容易混淆，誤以為網頁應用程式安全無虞了。

成功案例 References

AppScan全世界超過2000個客戶。台灣應用成功客戶不勝枚舉，精選案例如下: (所有案例僅限IBM內部參考用，請勿隨意亂發)

1. 法務部: 資訊部QA人員，管理委外開發系統。
2. 工研院: 幫政府部門開發軟體，上線前交由電算中心測試後，再交給政府單位上線。
3. 北縣府: SEIM平台建置，確認上線的應用系統安全性。
4. 師範大學電算中心: AppScan建置前內部僅登計110個網站，透過Appscan掃描後發現漏登100個網站。
5. 尚有淡江大學電算中心等十多家大專院校電算中心已購買。

AppScan 急救包 單機版軟體 + 產品安裝與使用說明 –
超值優惠價：新台幣109萬

DataPower：Web Service 安全方案

企業挑戰

當企業邁向SOA整合環境，XML及Web Services將會扮演其中最重要技術腳色。然而不同資料間轉換，XML解析，Web Services執行效能或安全性及管理機制，是大多數IT經理和架構師邁向SOA即將面臨的一個主要挑戰！

- 正在考慮或使用SOA/ Web Service XML運用!
- 需要加密、解密或數位簽章與驗章安全的解決方案!
- 正面臨著將現有大型主機應用系統與SOA/ Web Service 系統連接的難題
- 正面臨著XML訊息格式轉換的難題？

核心價值-產品功能

1. **Web 服務安全支援與存取控制:** 支援SAML及WS-Security可控制內外部用戶端對 Web 服務應用程式的存取權並且能整合 LDAP以達到授權認證之功能。
2. **XML Denial of Service (XDoS) 保護:** 能防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。如Single-message XDoS與Multi-message XDoS惡意攻擊
3. **XML 訊息加密與解密 Encryption/Decryption:** 可執行各種基本的 XML加密、解密、數位簽章，即可將*整個XML訊息或只將文件內某一個XML欄位*加密/解密及簽章/驗證。
4. **XML/SOAP 防火牆功能** 支援過濾 XML 及 SOAP 資料流量，可防止惡意使用者及型態異常資料破壞企業的應用程式伺服器或營運。

“專” 攻解決方案 Solutions

Data Power SOA 設備是業界*第一*個提供硬體解決方案的*市場領導者*

提供更安全SOA環境

-提供與外在系統連線時，系統間資料傳輸安全。如加密、解密或數位簽章與驗章

簡化SOA部署與快速整合

-利用革命性的技術在二進位文字及 XML 訊息格式之間轉換與繞送。協助實現安全的企業訊息匯流及系統整合。

加速 XML 處理程序

-可將常見的XML處理從伺服器或系統中卸載(offloading)下來進行加速，可加速大量的XML資料處理通常可有倍速效果

加強SOA治理 (Governance)與政策 (Policy)

-可擷取和連結 WSRR的服務，定期更新 Cache且針對服務擷取變動並執行時期原則與安全。

成功案例 References

客戶證言

「導入DataPower後，處理速率就明顯改善，現在處理過去兩、三倍的資料量都沒問題：其次，DataPower可協助在訂單資料進來及出去前先進行XML的格式驗證，一旦錯誤就直接擋信，此一驗證讓資料量大的公司可節省人力成本。」～宏碁集團資訊技術總處　資訊長　李文進

專案效益

1. 大幅增加系統整合與開發的生產力
2. 減少系統開發、測試時間、專案建置風險與導入期間並減少系統上市時機
3. 增加系統處理效率與系統處理資料量二~三倍
4. 增加擴充性和穩定性

WebSphere DataPower XI 50 定價 NT$ 1,950,000 (未稅)

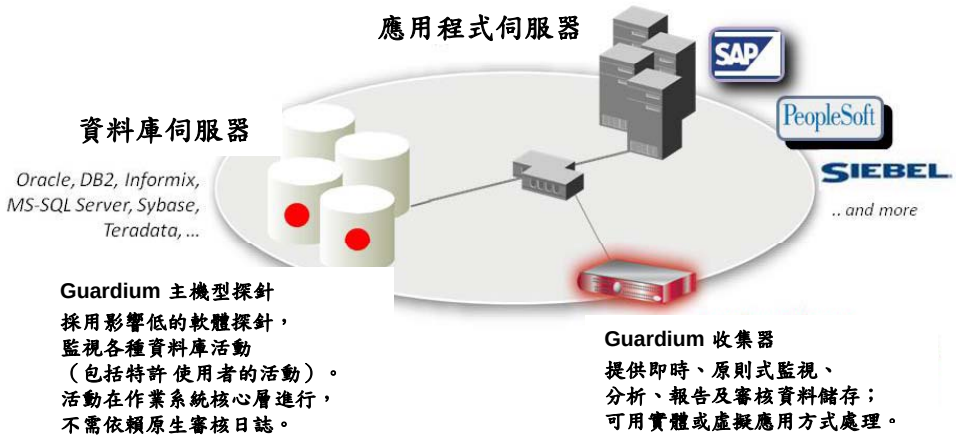
Guardium： 即時資料庫監控、保護、及法規遵循

您知道嗎？

- 75% 的資訊外洩是由資料庫伺服器造成。
- Guardium 可支援Oracle、SQL Server、DB2 UDB、DB2 for z/OS、DB2 for iSeries、Informix、Sybase、MySQL、Teradata。
- Guardium 的使用者包括全球前五大跨國銀行，全球前三大跨國零售商其中兩間，全球前六大保險公司其中四間，兩大全球最受歡迎飲料品牌和各大知名企業如Dell 、Accenture 和 McAfee.com。
- 法規遵循的最大重點在於 SOX（保護 ERP/財務系統），接下來是 PCI（智慧卡持有者資料）以及資料隱私。
- 對於財星五百大企業而言，Guardium 的投資報酬率為 239%，僅需 5.9 個月便能回收投資（Forrester 個案研究）
- Forrester 研究將 Guardium 譽為「本領域龍頭」，在「現有產品與服務」、「架構」及「產品策略」均為第一。
- 一般的企業交易額為25萬至100萬美元，而客戶若擴展到其他業務單位及應用，便會大幅增加附加交易。
- 一般服務： 安全、遵規或風險目錄； DBA； 應用程式架構； SOX 專案 經理； 基礎架構經理。
- Guardium 可專門著重監控資料庫層，輔助 IBM TCIM、TIM/TAM、及 ISS Proventia。
- Guardium 可支援異質的資料庫環境，輔助 IBM AME。

適用問題： 您是否需要以下動作？

處理因資料庫控管不善而導致的審核問題。
為遵守沙賓法案 (SOX)，避免有人未獲授權而更改財務資料。
監控特許使用者，並實行職權分立。
避免資料外洩（例如 SQL 資料隱碼攻擊）。
找出資料庫的漏洞和遺漏的修補程式。
找出詐欺行為（使用 SAP、PeopleSoft、Oracle e-Business 等等）
減少遵規所需的人力和時間（各項法規如 SOX、PCI、NIST、FISMA、EU DPD、ISO 27002、資料隱私法等等）。*競爭對手*：
Oracle、Imperva、AppSec、Netezza/Tizor、Secerno、Sentrigo、Idera、Lumigent、NitroSecurity、Fortinet



輕鬆完成資料庫監控及法規遵循

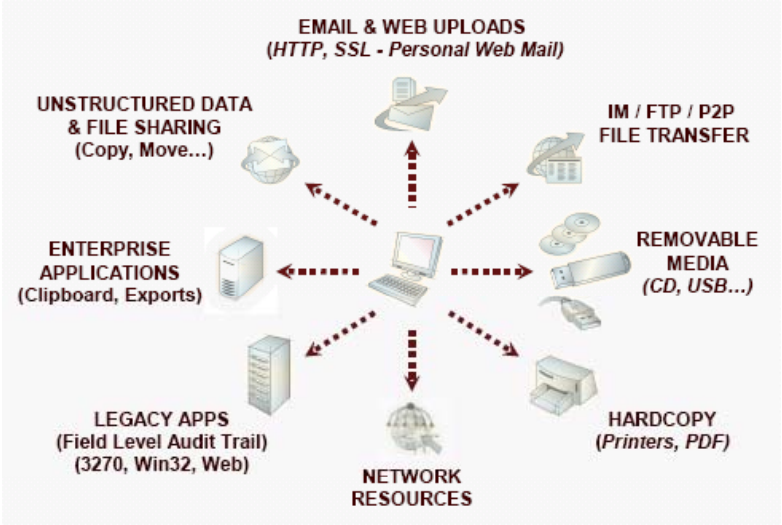
產品主要特色

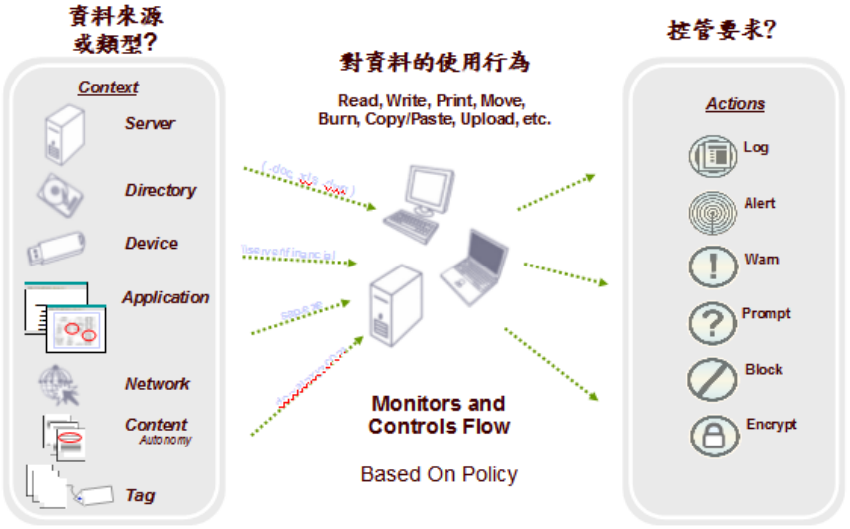
1. 非侵入性： Guardium 可持續即時監控所有資料庫行動，但不需改變資料庫或應用程式配置，也幾乎不會影響效能表現。
2. 異質性： 支援各主要 DBMS 平台。
3. 降低作業成本： 自動化處理各種法規遵循報告及監管程序（6 個月內回收成本）。
4. 擴充性： 例如 Dell 已在全球 10 個資料中心超過 1000 台資料庫伺服器上部署 Guardium 以遵守 SOX、PCI 和 SAS70 等法規。 Guardium 具備多層式架構、網路管理主控台、集中處理的跨 DBMS 稽核儲存庫，能夠達到集中處理的目標。
5. 職權分立： 審核資料儲存於多個不同的實體或虛擬裝置中，內部人員或是駭客無法藉由篡改審核日誌資料來遮掩不法情事。這種作法不需仰賴原生的審核日誌（常駐於 DBMS 中），因此不需擔心被管理員輕易改動，便能確定職權分立。

資料洩漏保護方案Data Loss Protection簡介

- 針對內部使用者進行機敏資料保護與行為稽核

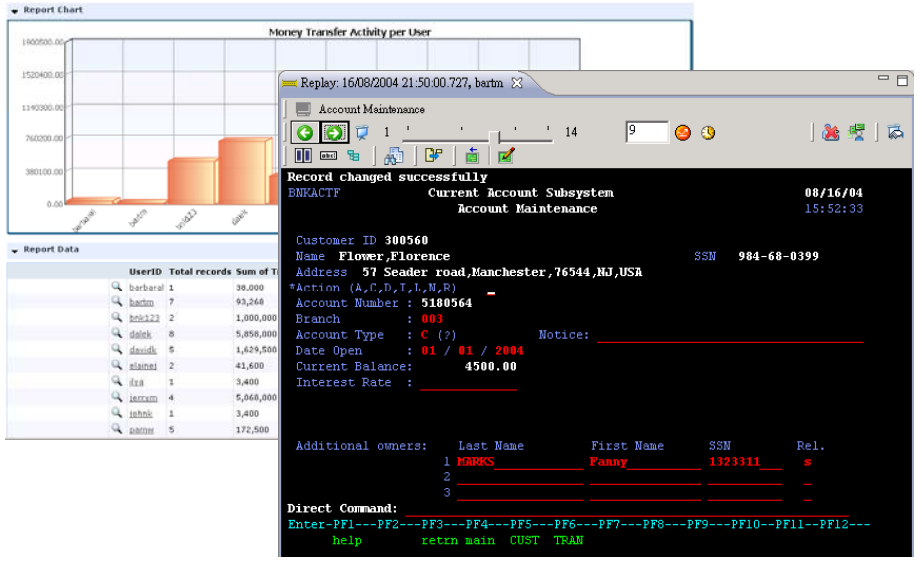
- 文件使用監控與保護強化 – 監視/控管機敏資料之使用行為, 必要時可直接阻擋特定行為, 同時維持使用者對資料之使用存取能力
- 降低維運成本 – 建立機敏資料之使用報表及稽核, 提供完整不需客製化之報表介面, 可協助快速進行決策支援
- 強化機敏資料存取之可見度 – 辨識及紀錄資料在群組及使用者間的移動及使用狀況
- 完整保護機敏資料生命週期 – 完整保護及紀錄機敏資料，文件進行複製/更名/內容擷取等動作時，機敏資料仍能被認出及保護

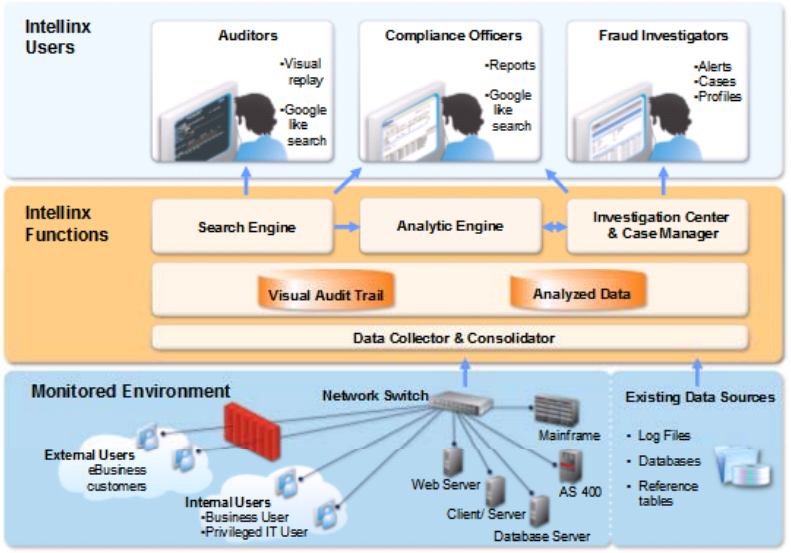




使用者行為稽核方案簡介
- 強化用戶行為操作稽核，遏止惡意使用者外洩個資

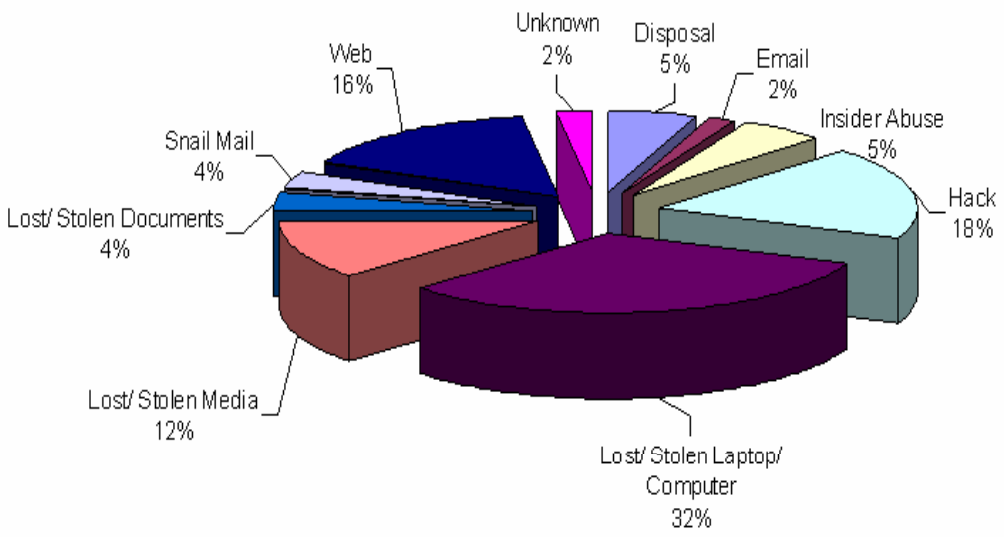
- 擷取並顯示內部使用者之交易行為
  - 針對3270 / 5250 / VT / HTTP / DB / MQ等交易封包進行擷取並儲存
  - 可將交易資料重組，重現交易員操作之畫面，支援操作過程的完整重播
- 針對交易輸入及輸出內容進行搜尋
  - 可透過關鍵字進行交易搜尋，提供彈性的資料搜尋能力
- 支援企業定義之商業稽核規則
  - 支援自定義稽核規則，從維運或業務角度出發，對觸發規則的操作行為觸發告警或其他定義的動作



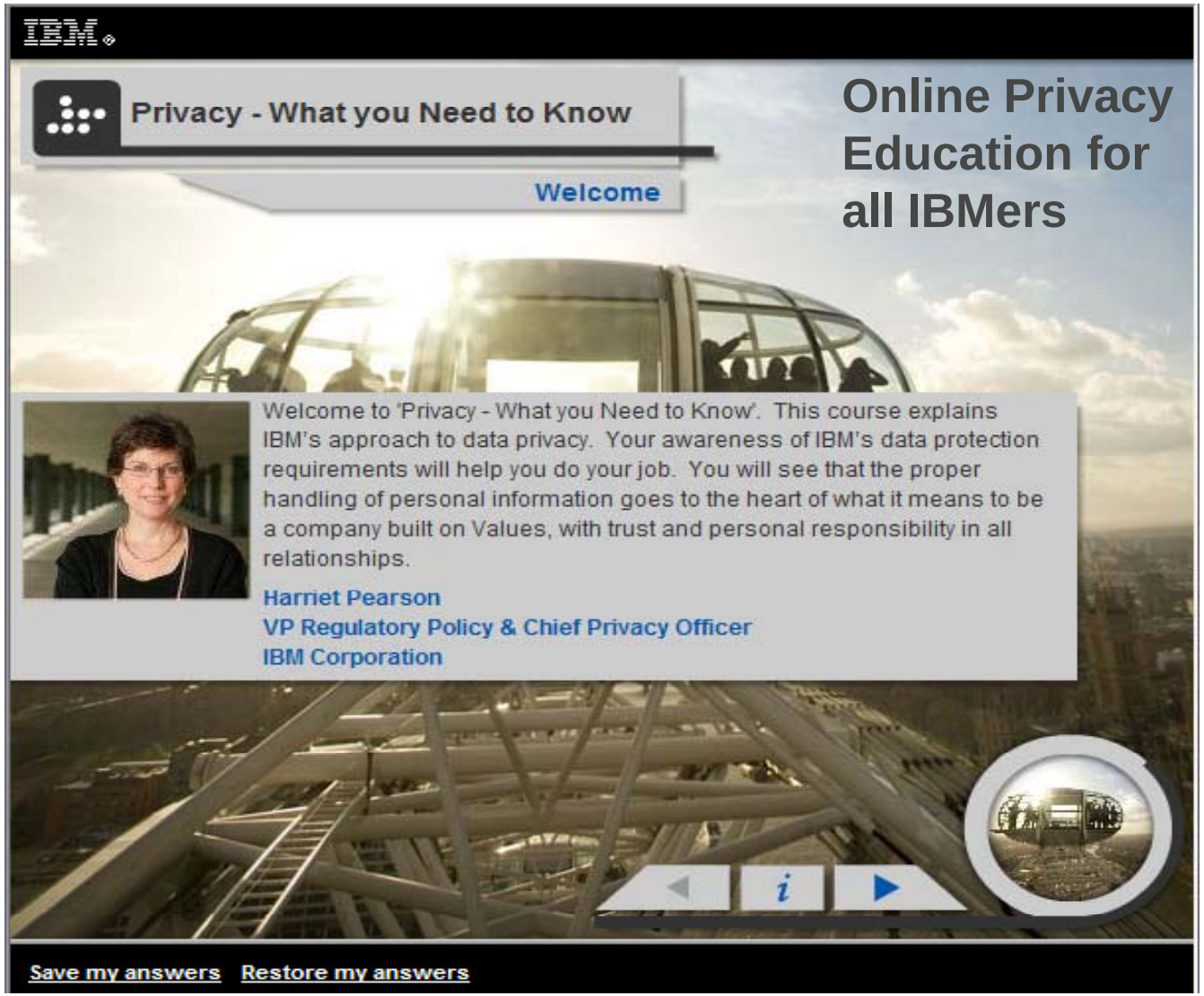


端點硬碟加密方案簡介
- 保護個資及機敏資料免於行動設備遺失及遭竊

- 完整之使用者硬碟加密保護 – 透過集中的管理機制硬碟進行完整加密保護以強化資料安全
- 加速部署 – 簡化的導入過程，提供和既有系統最大的相容性
- 使用者經驗 – 使用完全透明化，不影響使用者日常作業。End-user幾乎不需要教育訓練即可使用，日常運作時幾乎沒有任何performance loss
- 完善的Recovery機制 – 完善的中控機制提供於使用者忘記密碼，以及PC/Notebook損壞時的資料回復作業



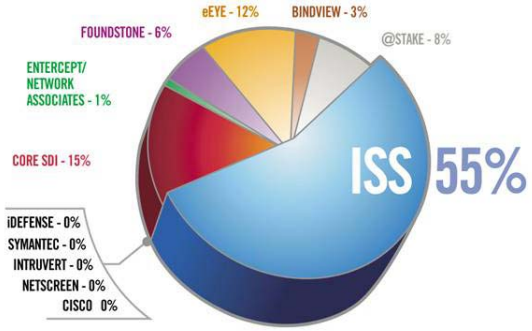
政策及制度需透過持續不斷的教育訓練及宣導才能達到執行效益



在IBM ISS X-Force® 研發團隊的支援下，於全球擁有多座資安研發實驗室及安全監控中心(SOC)

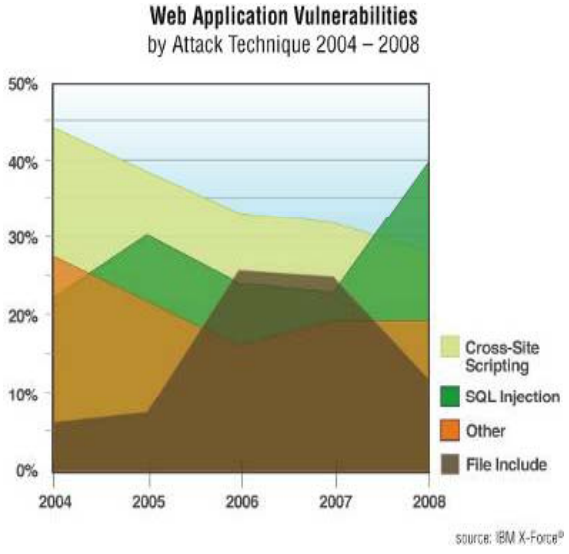
X-Force 是全球頂尖的企業級安全研發團隊

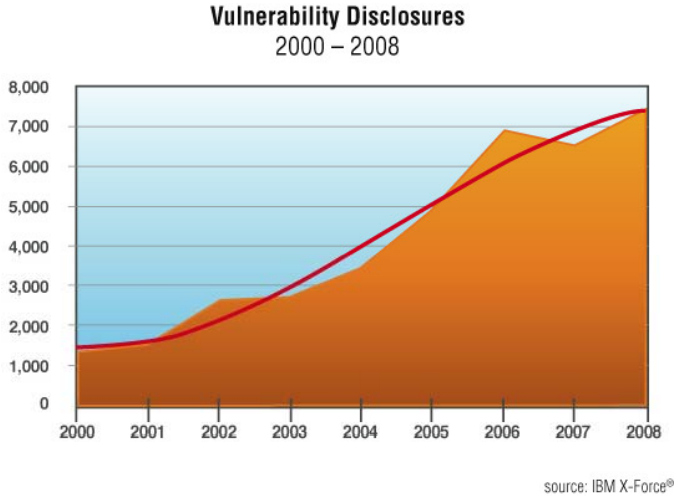
- 長達14年的研發歷史
- 專注于發現和分析安全風險，開發技術對策
- 每半年發佈一次網路整體風險趨勢狀態報告
- 每年發佈30 次以上的安全建議和警告
- 每月找出200 多個新的攻擊手法
- 維護超過 38,000 個漏洞的安全資料庫
- 開發了 6000 多個檢查項用於檢測和發現攻擊手法
- 發佈X-Force月度威脅觀察報告 (XFTIM)
- 2008年，研究與發現7406個安全漏洞
- CVE組織創始人之一，相容CVE/CPE/CVSS

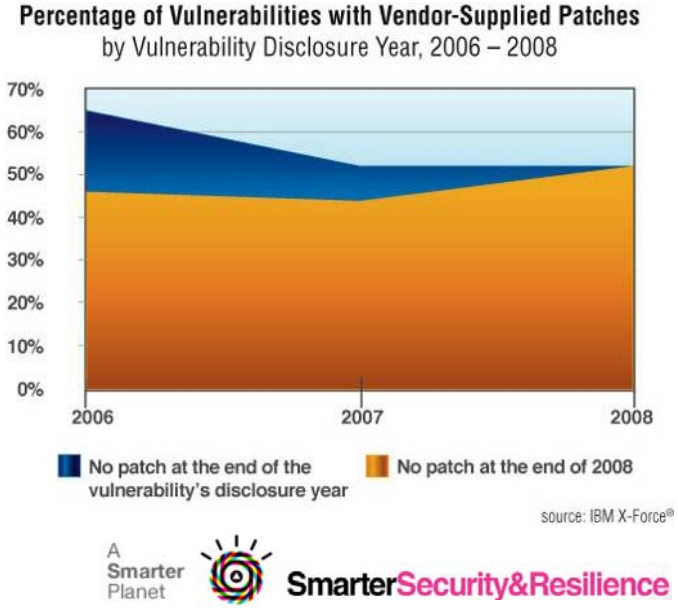


高風險漏洞發現比例

Frost & Sullivan 2006 , Internet







A Smarter Planet

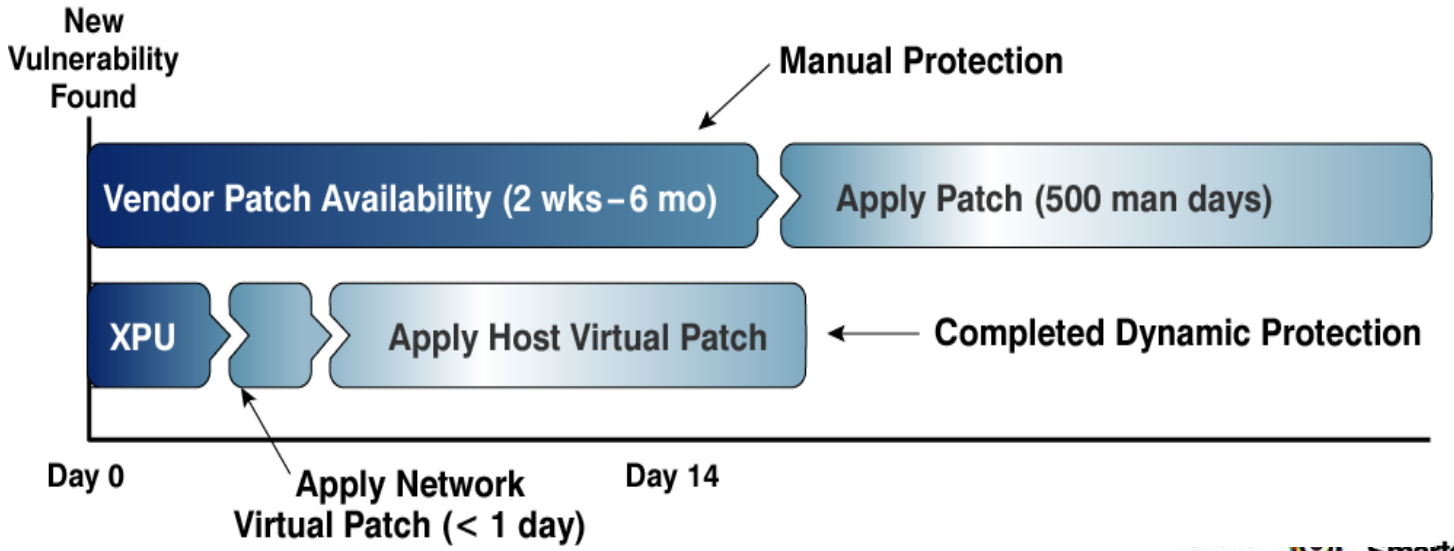
SmarterSecurity&Resilience

IBM ISS 核心價值- Virtual Patch 虛擬補丁

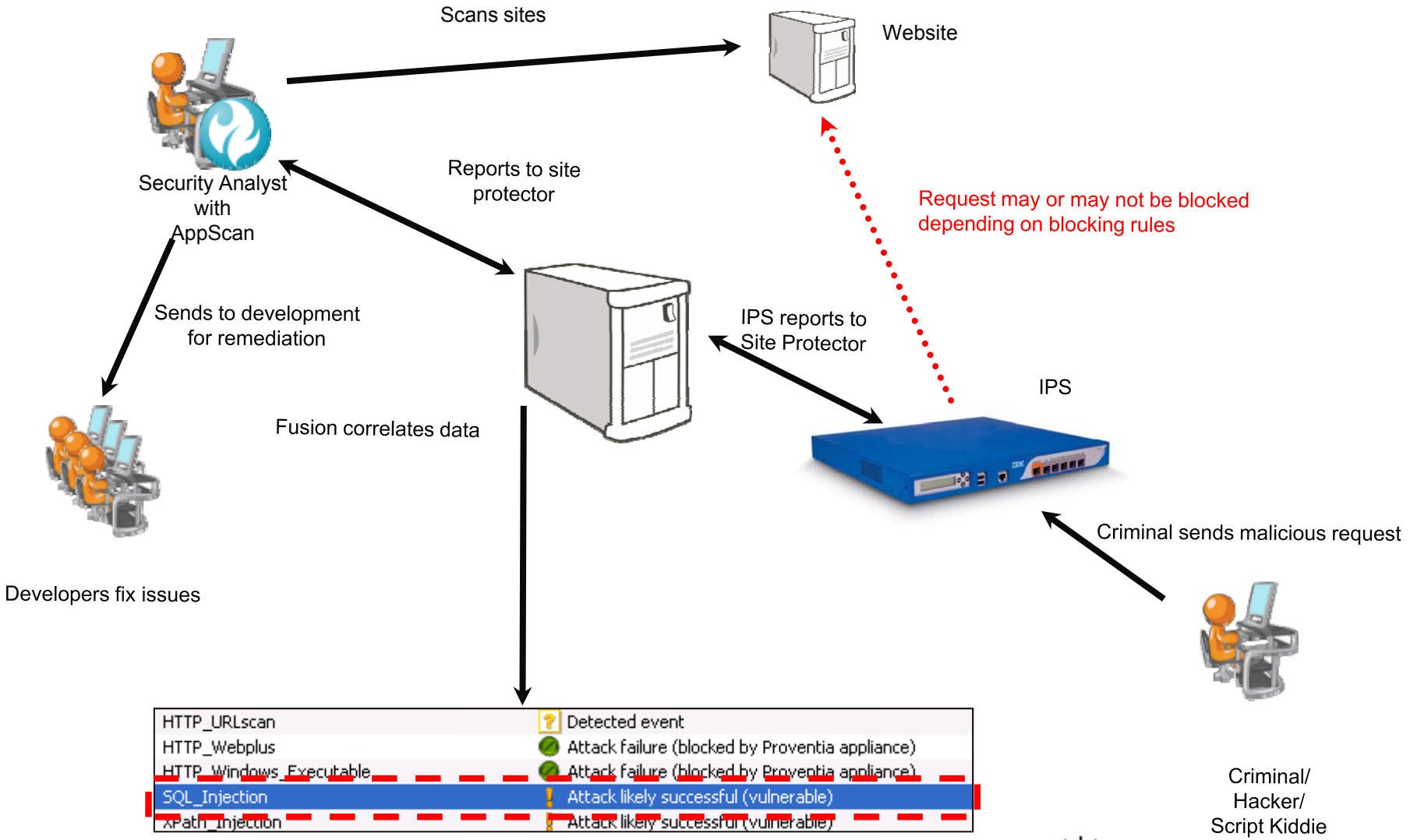
Virtual Patch 為面臨最新漏洞威脅的企業提供了充分的 時間緩衝 ，在系統和應用廠商就新漏洞提供補丁和更新之前，防止漏洞被利用，同時也可避免補丁與業務應用衝突的風險，確保企業的安全。

為什麼能夠實現前瞻性保護？（Proactive Protection）

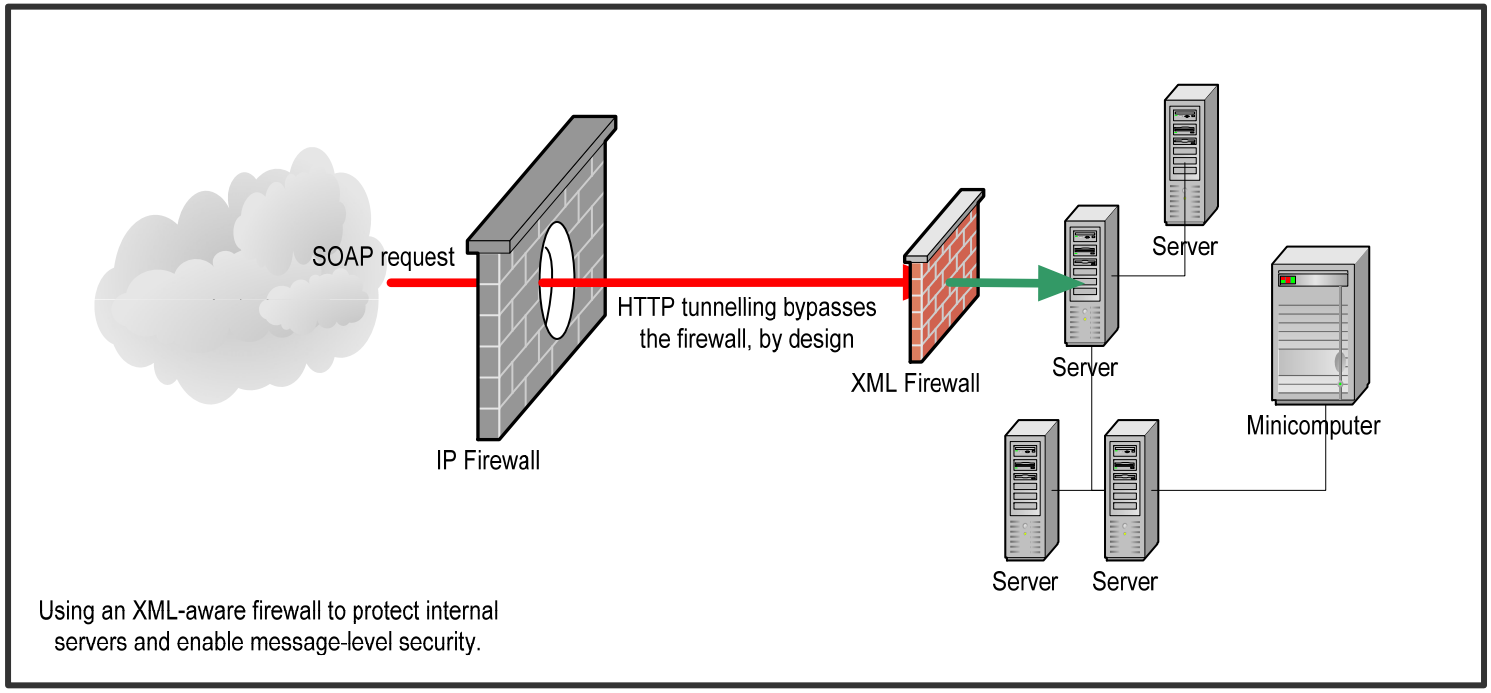
由於IBM ISS首先發現的高危漏洞最多，同時，和系統廠商保持了雙贏的合作關係，所以有能力在漏洞被發現的第一時間提供針對漏洞本身的防護，而非提供針對攻擊的防護。因此，無論攻擊手法和利用程式如何變化，ISS提供針對高危漏洞的前瞻防護。



IBM AppScan 與 ISS 完美的結合：應用程式安全檢測與網路安全防護的整合



在XML/Web Service 應用中，WebSphere DataPower SOA Appliances可保護應用程式不受未經授權存取與惡意訊息的侵害，提供完整的安全資料交換機制。



- 應用設備達到最高安全等級
- 應用設備加速加解密速度
- 支援高等級的加密演算法
  - –Encryption algorithms: 3DES, DES, AES
- 較低的**TCO** 與最佳 **ROI**

IBM提供全面向，由顧問服務至產品導入之完整資料保護服務，由IBM資訊安全專家帶領整個專案之完善進行，並確保專案內由前期顧問服務與規劃至產品佈建之知識完整轉移