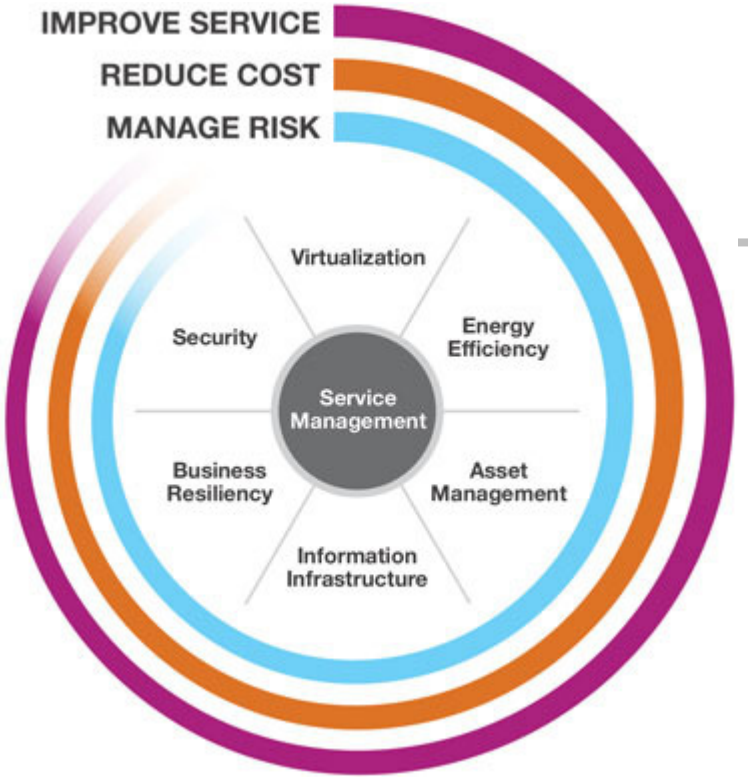
因應個資新紀元:【企業錦囊妙計分享會】

妙計二：資料外洩分析與處理



林育震 Julian Lin
台灣IBM技術總監

A Smarter Planet

SmarterSecurity&Resilience

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

法規要求	IBM解決方案套餐	IBM 解決方案	產品對應
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 ■ 開發測試階段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

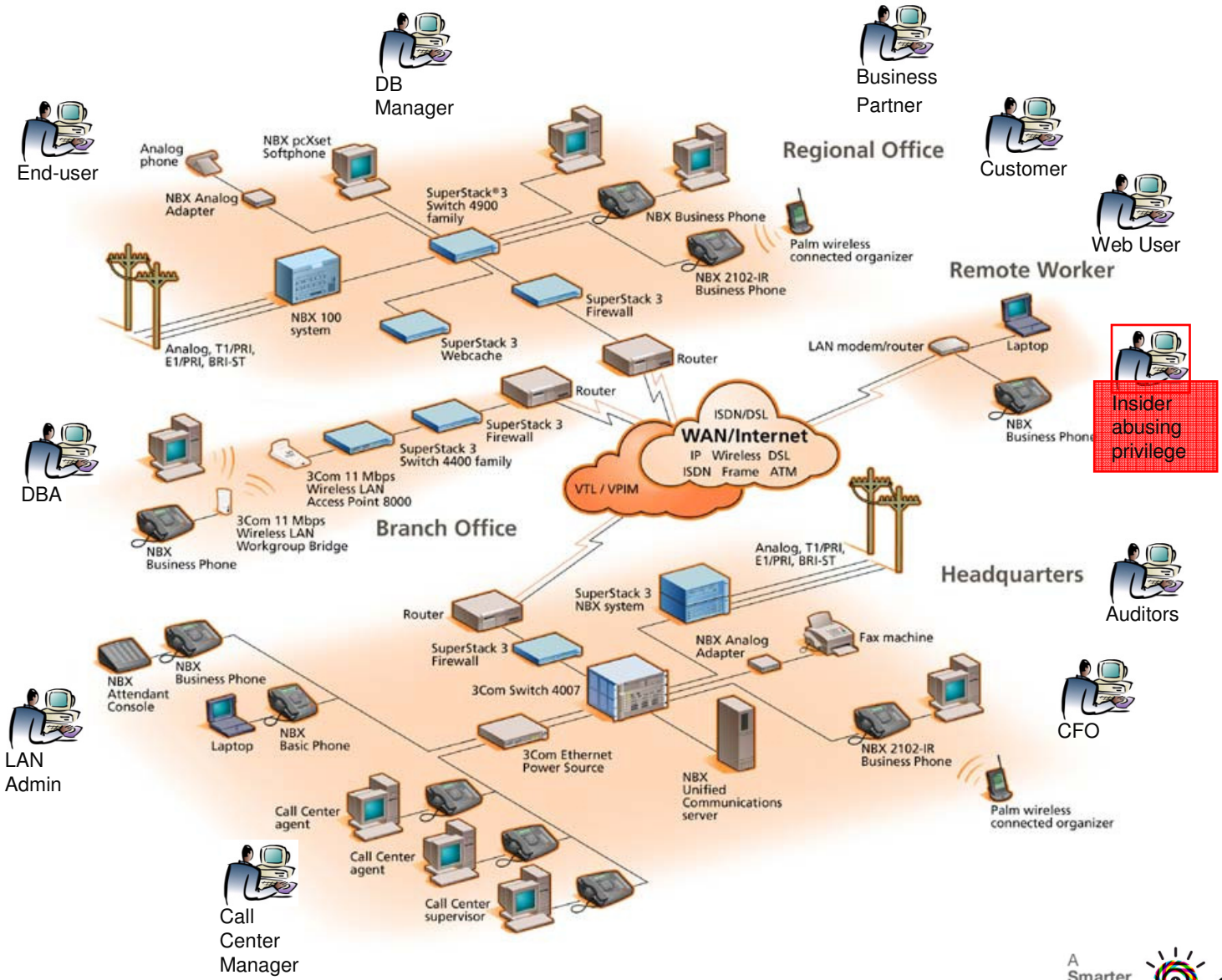
Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 作業風險與內部稽核的挑戰
- 系統架構與功能
  - 內部使用者行為稽核
  - 日誌集中管理及分析
  - 資料庫稽核與防護
- 方案應用範例
- 效益與總結

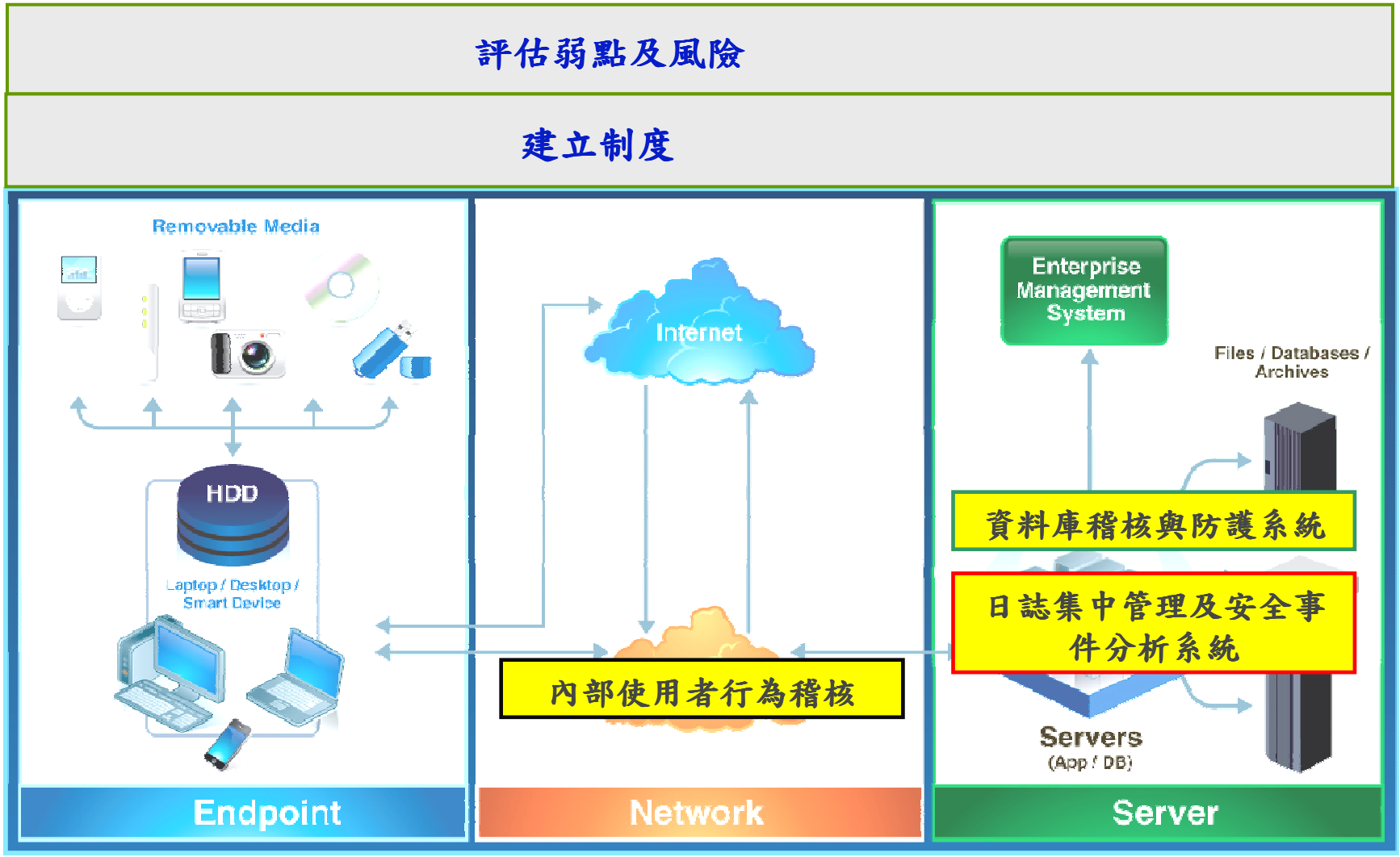
有哪些使用者在你的網路中做什麼事? 您如何稽核?



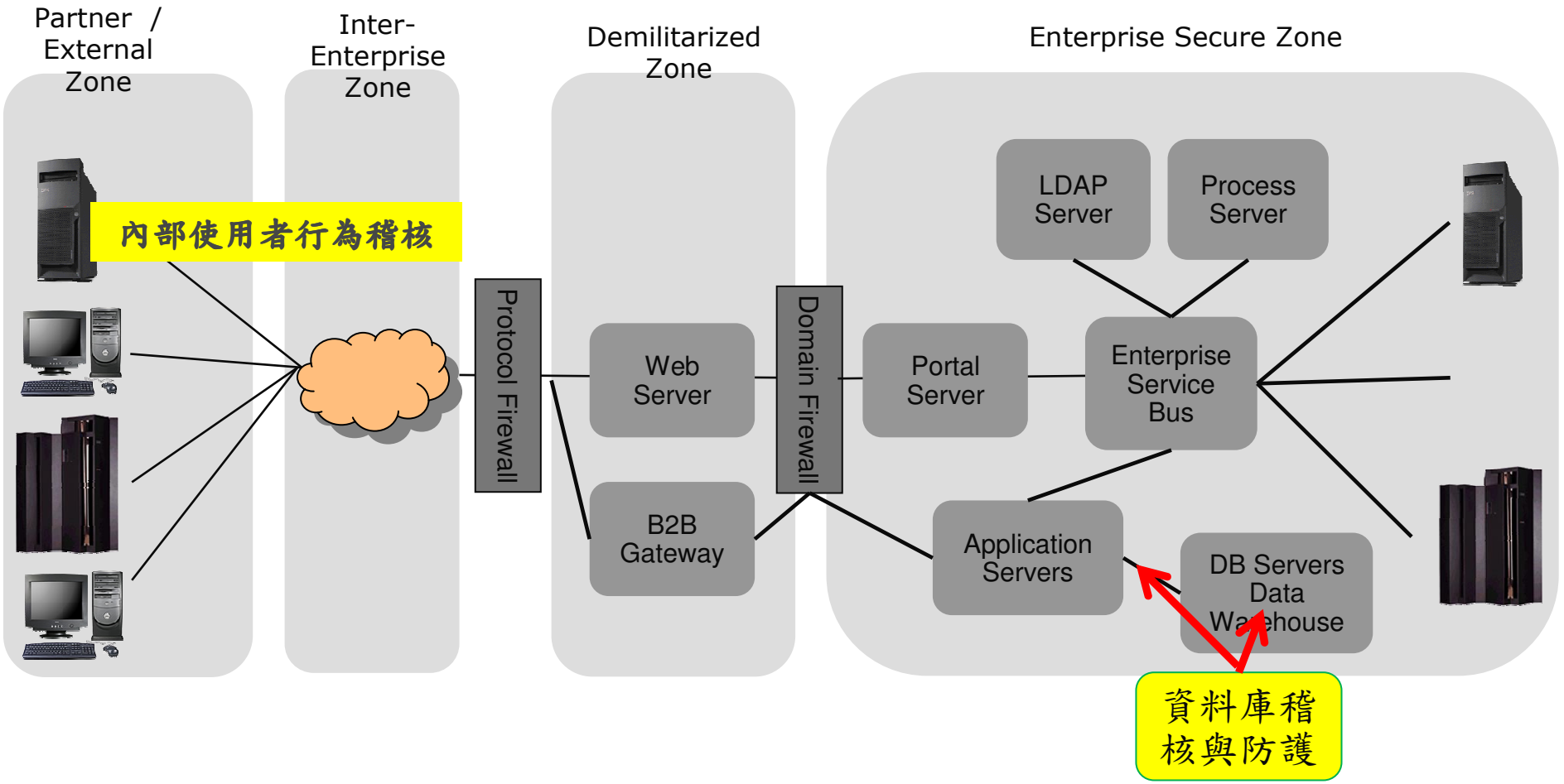
安全問題:

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

在IBM的整體協助方案「資料外洩分析與處理」中關心的是：使用者在畫面上打了什麼字？系統回應了什麼？漏失的資料時由哪個關卡出去的？有沒有不正常的行為模式？是誰在何時經由哪個節點存取了資料庫的什麼資料？能不能及時阻擋？



IBM資料安全解決方案實體架構圖 – 資料外洩分析與處理 – 重點在稽核，也包含阻斷



日誌集中管理及安全事件分析系統

稽核的對象 - 企業相關的授權用戶操作風險的來源，包含業務人員的日常操作及特權用戶的日常維護

- **業務人員的日常操作（業務層）**

  包括客服中心人員、打單人員、櫃台人員、業務專員、交易室、信用卡部人員等

  - 惡意欺詐行為（篡改餘額或客戶資料、竊取並出售客戶個人資訊）
  - 外來因素引發的敏感操作－洗錢、巨額轉賬

- **特權用戶的日常維護（IT系統層）**

  特權用戶：系統管理員、資料庫管理員、操作員、QSECOFR、IBMUSER、RACFADM、root等

  - 失誤操作導致關鍵應用伺服器異常甚至當機
  - 違規操作導致系統上的敏感資料資訊丟失或破壞
  - 惡意操作導致敏感資訊洩漏（如客戶資訊，帳戶資料等）

端點的稽核 - 內部使用者行為稽核 - 如何發現內部用戶違規操作的挑戰

- 如何從操作行為角度監控使用者的行為模式？
- 是否能提供重播功能，真實還原違規行為的操作過程？
- 除了內部使用者更新的行為外，針對僅查詢個人資訊的唯讀行為是否能夠稽核？
- 是否能有好的搜尋方式，以快速查詢到事件發生點？
- 是否具備跨平臺的稽核能力？
- 對所有用戶包括特權用戶的行為都能稽核？
- 是否可以用合理的儲存量，儲存大量且長時間的內部用戶操作資料？
- 稽核系統建置時，是否可以不影響營運系統的效能與可靠度，也不影響用戶的操作行為？

並不是所有事件都在端點發生
端到端的稽核 - 日誌集中管理及安全事件分析的挑戰

- 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？

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

- 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?

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

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

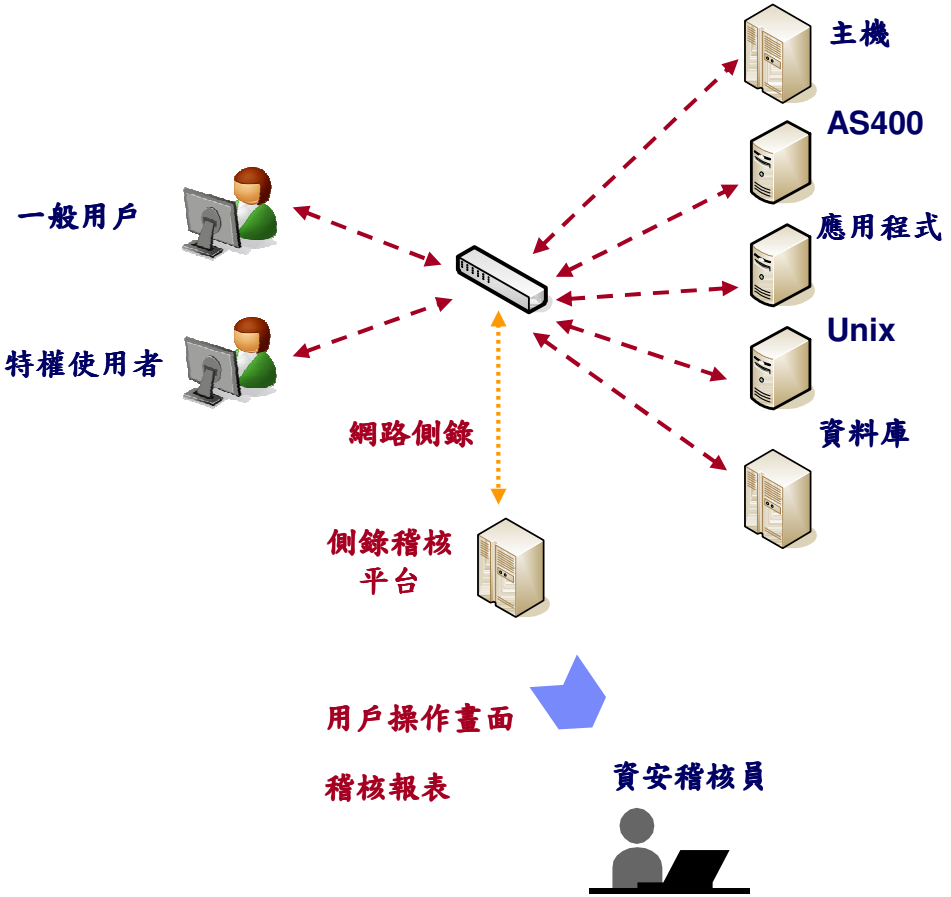
Agenda：

- 作業風險與內部稽核的挑戰
- 系統架構與功能
  - 內部使用者行為稽核
  - 日誌集中管理及分析
  - 資料庫稽核與防護
- 方案應用範例
- 效益與總結

內部使用者行為稽核的功能需求，要能支援跨平臺且不影響系統效能

- 採集並**完整記錄用戶操作的過程，包含用戶的查詢與更新操作**
- 支援主流通訊協定，解析螢幕或資訊欄位並儲存到資料庫
- 能夠**重組螢幕或資訊，支援操作過程的完整重播**
- 提供**快捷靈活的查詢功能**
- 如果一個用戶操作涉及多個螢幕，能夠連續分析並識別
- **從維運或業務角度出發支援自定義稽核規則，**對觸發規則的操作行為觸發告警或其他定義的動作
- 支援**跨平臺的稽核**
- 採用獨立設備**以被動式監聽方式進行用戶操作紀錄，佈建快速亦不需要更動現有用戶環境，**不影響系統效能
- 僅須**合理之儲存量**，可提供長時間與大範圍內之稽核資料儲存

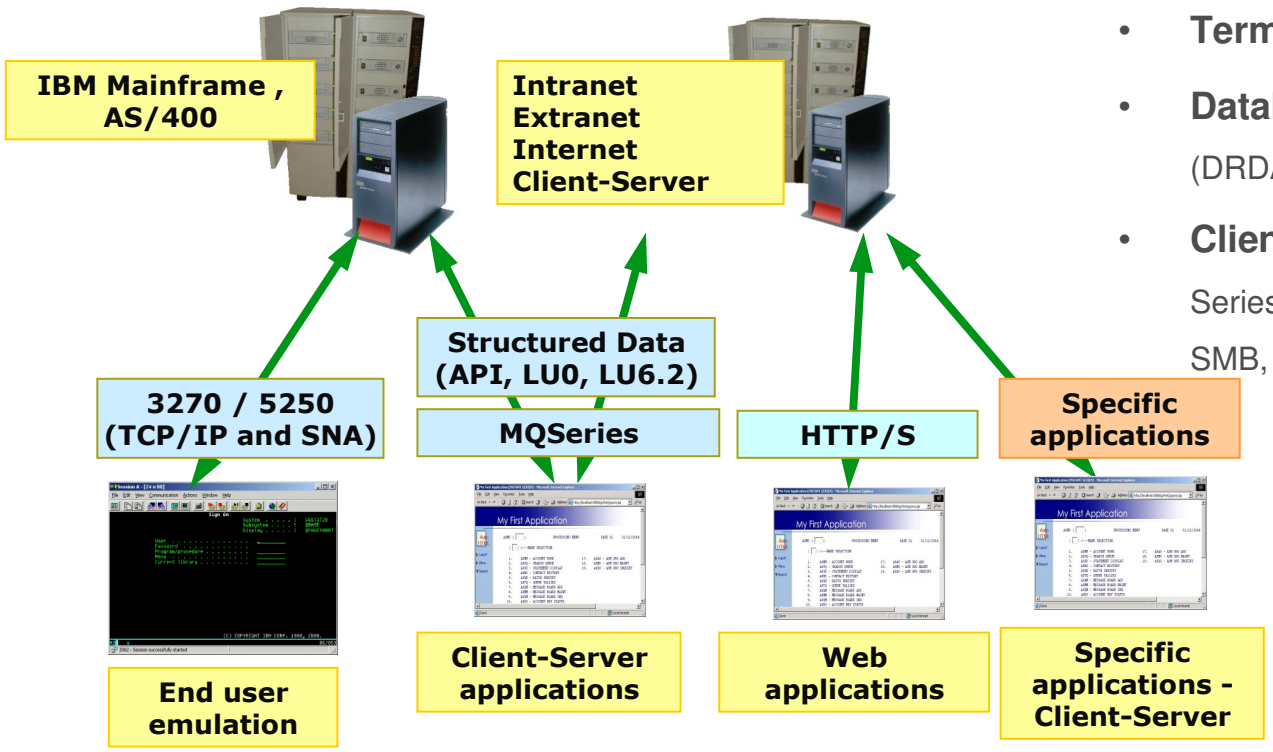
採用網路側錄進行內部使用者行為稽核的方式：不影響系統效能、重現操作畫面、跨平台的稽核能力



- **高效能、可靠度、與資料完整度**
  - ✓不影響系統效能與可靠度
  - ✓側錄資料無法被特權使用者修改
  - ✓不更動原有的用戶操作行為
- **可讀性高**
  - ✓重現用戶操作畫面
  - ✓直覺的稽核報表
  - ✓Google Like搜尋方式
- **跨平台的稽核能力**
- **低儲存量**
- **易於訂定業務或IT稽核規則**

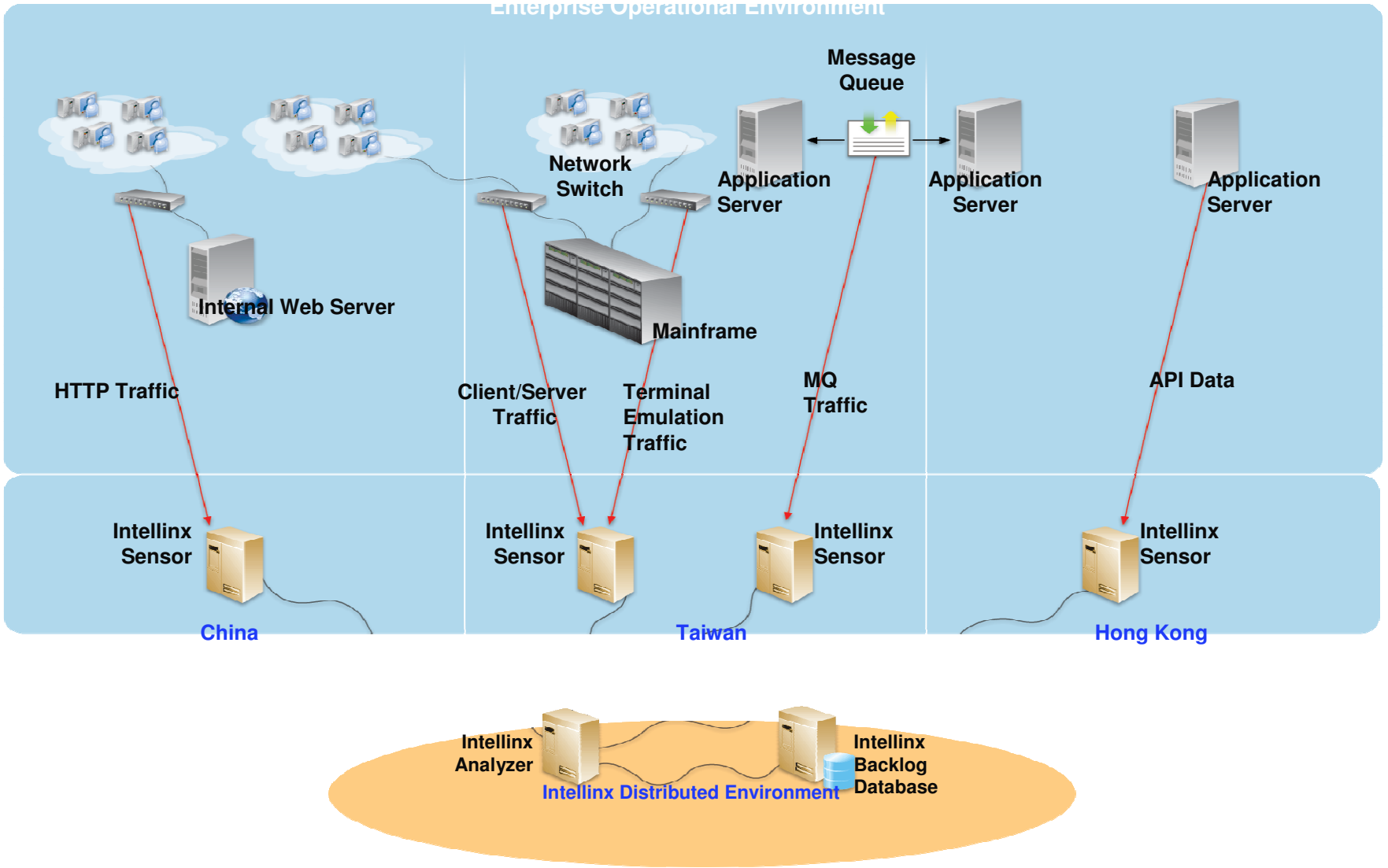
內部使用者行為稽核方案支援跨系統平臺與通信協定

Intellinx軟體

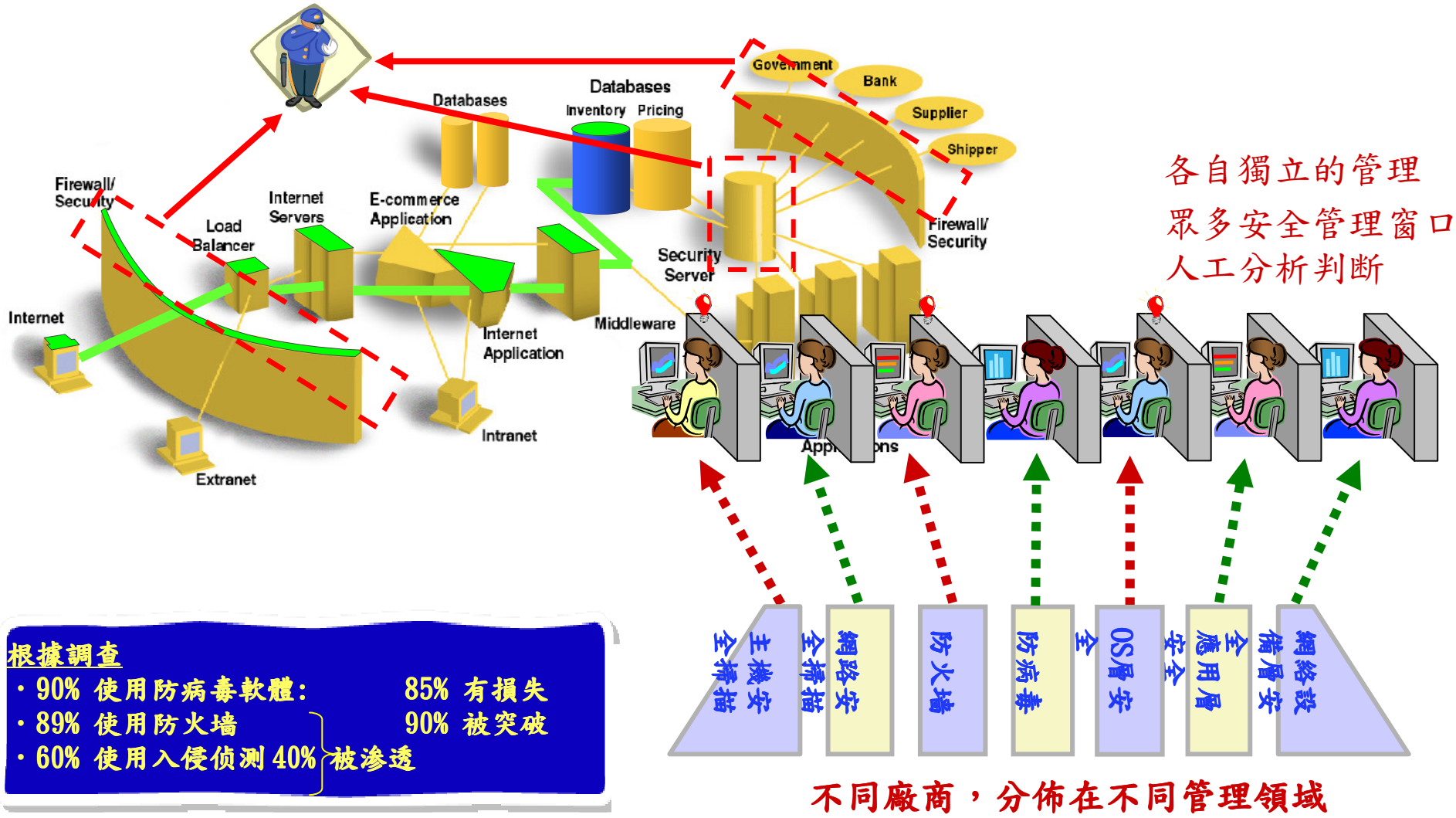


- **3270** – SNA, TCP/IP (TN3270), Enterprise Extender, SSL support
- **Unisys** - TD830
- **5250** – SNA, TCP/IP (TN5250), MPTN, SSL
- **Web Access** – HTTP, HTTPS
- **Terminal Access** – VTXXX protocols
- **Database access** – Oracle (SQLNET), DB/2 (DRDA) and MS SQL (TDS)
- **Client/Server messages** – TCP/IP, MQ Series ,MSMQ, mainframe SNA LU0 and LU6.2, SMB, FTP

偵測器可以配合部署在不同區域，由中心端來稽核與分析內部使用者行為



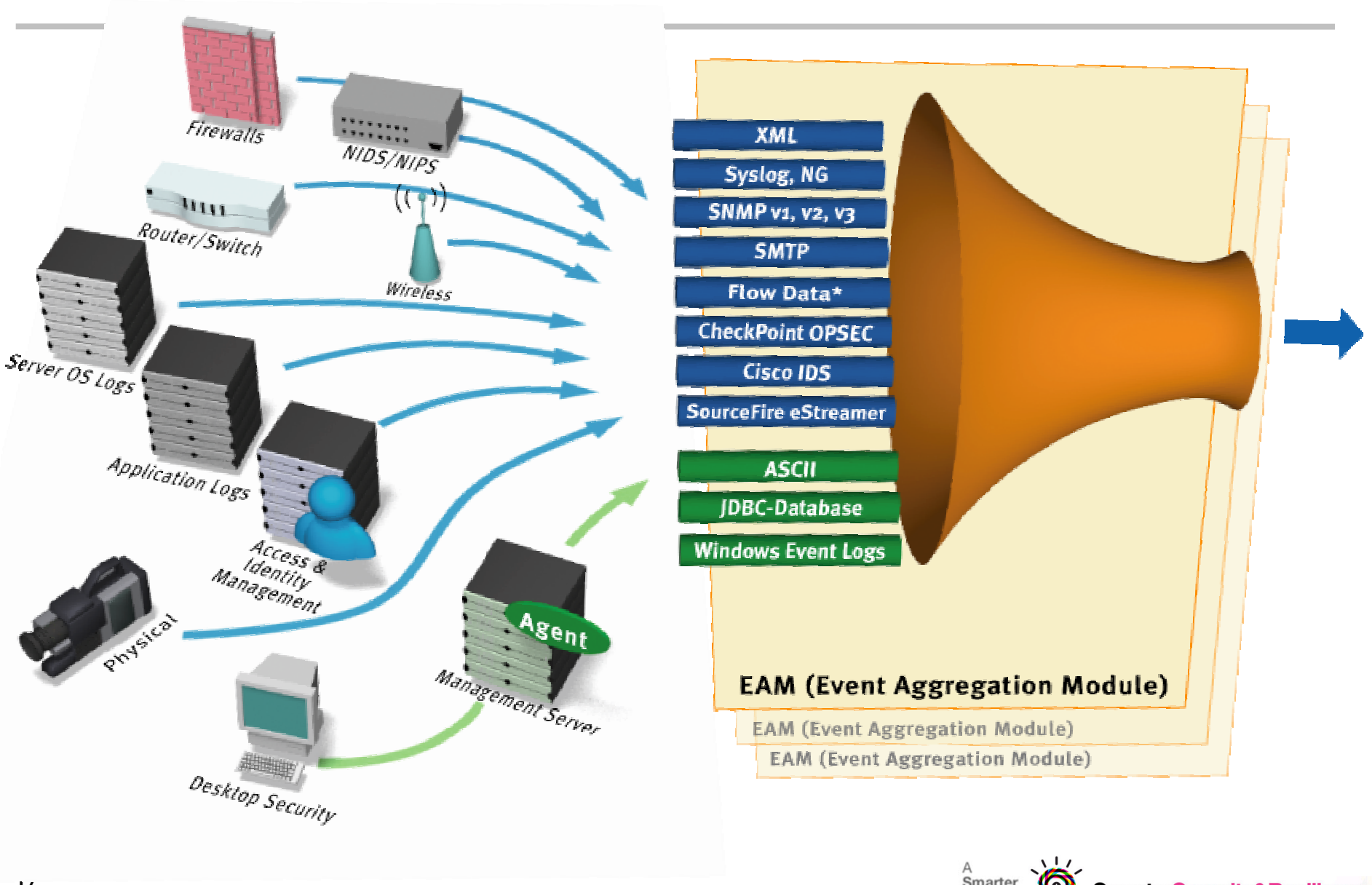
稽核與分析內部使用者行為之外，散布在各地的安全防護是否有達成預定的效果？是否能端到端綜合分析，證明已善盡保管人責任，並且找出問題點在哪裡發生



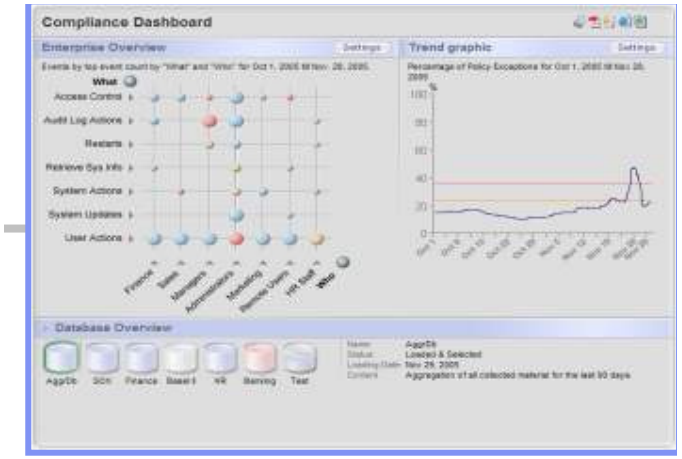
根據調查

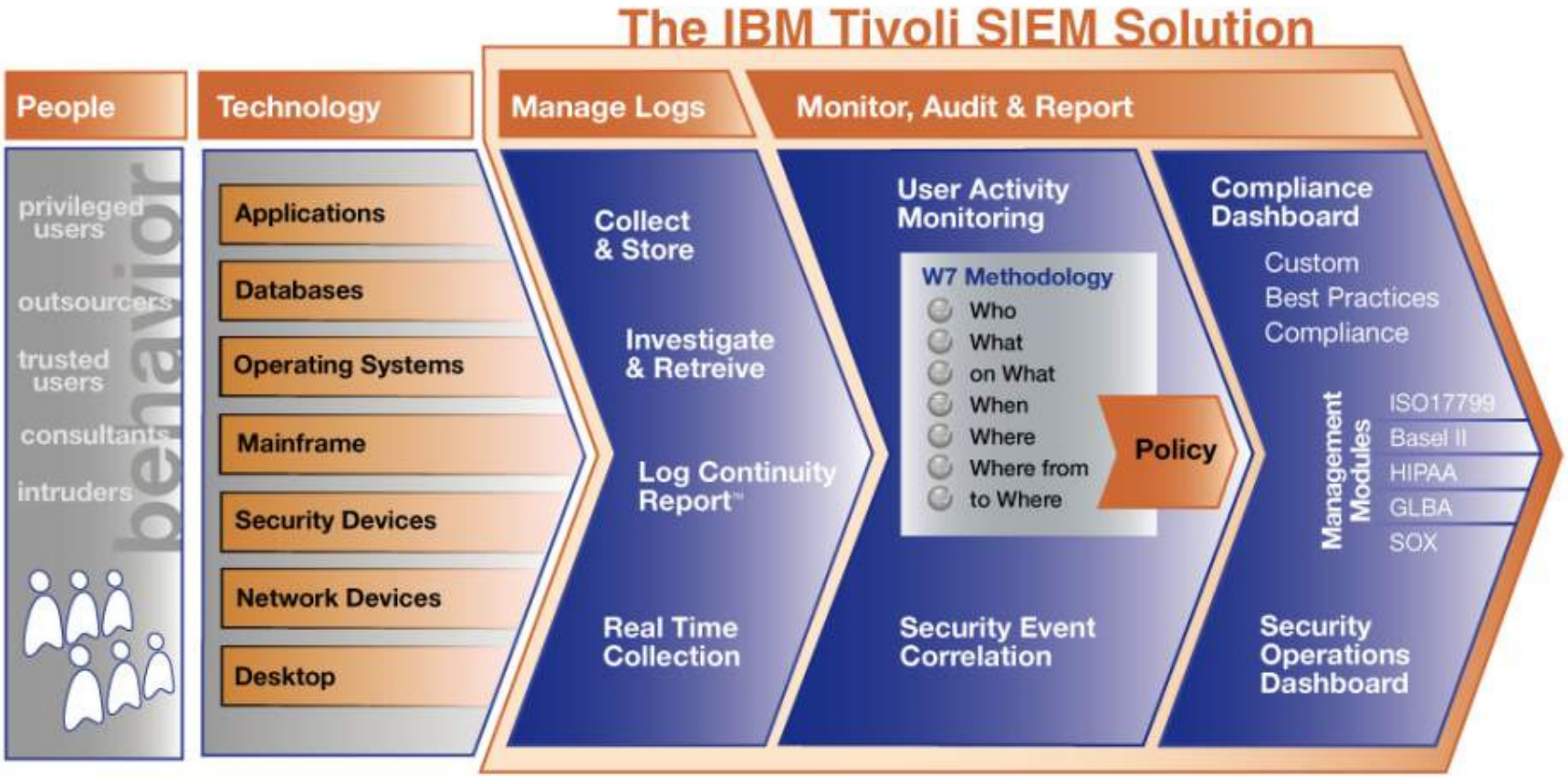
- 90% 使用防病毒軟體: 85% 有損失
- 89% 使用防火墻 90% 被突破
- 60% 使用入侵偵測 40% 被滲透

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



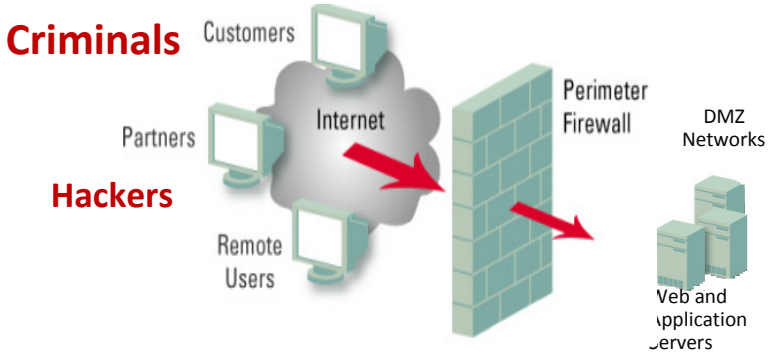
IBM日誌集中管理及分析方案能收集Desktop、Network Devices、Security Devices、mainframe、OS...等的日誌，將安全事件關聯起來，產生各種合規報表，並隨時反映在儀表板上

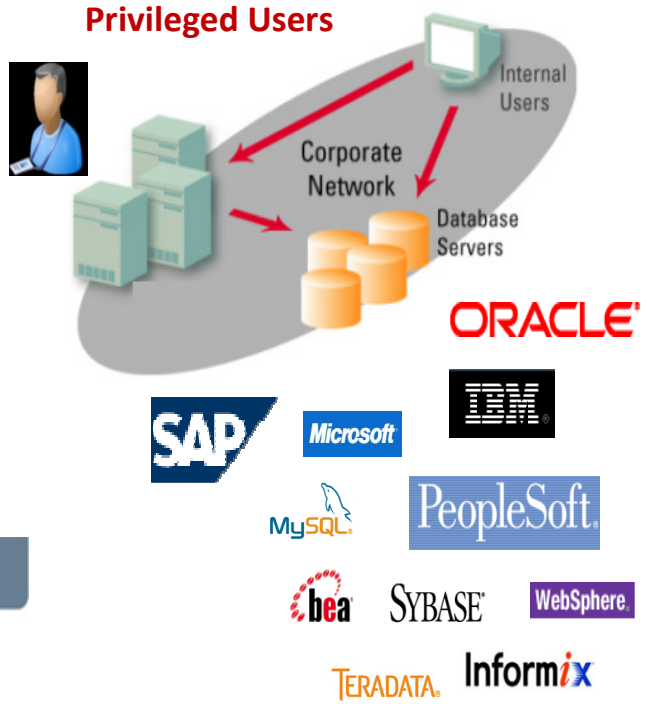


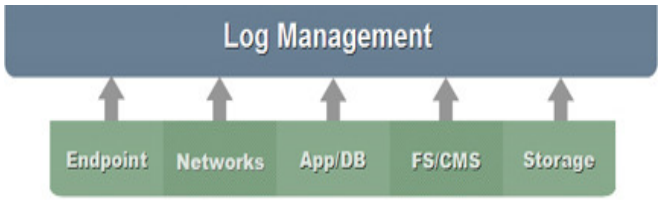


但是有一些行為是系統日誌上沒有記載的，例如SQL指令的內容

- 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.)

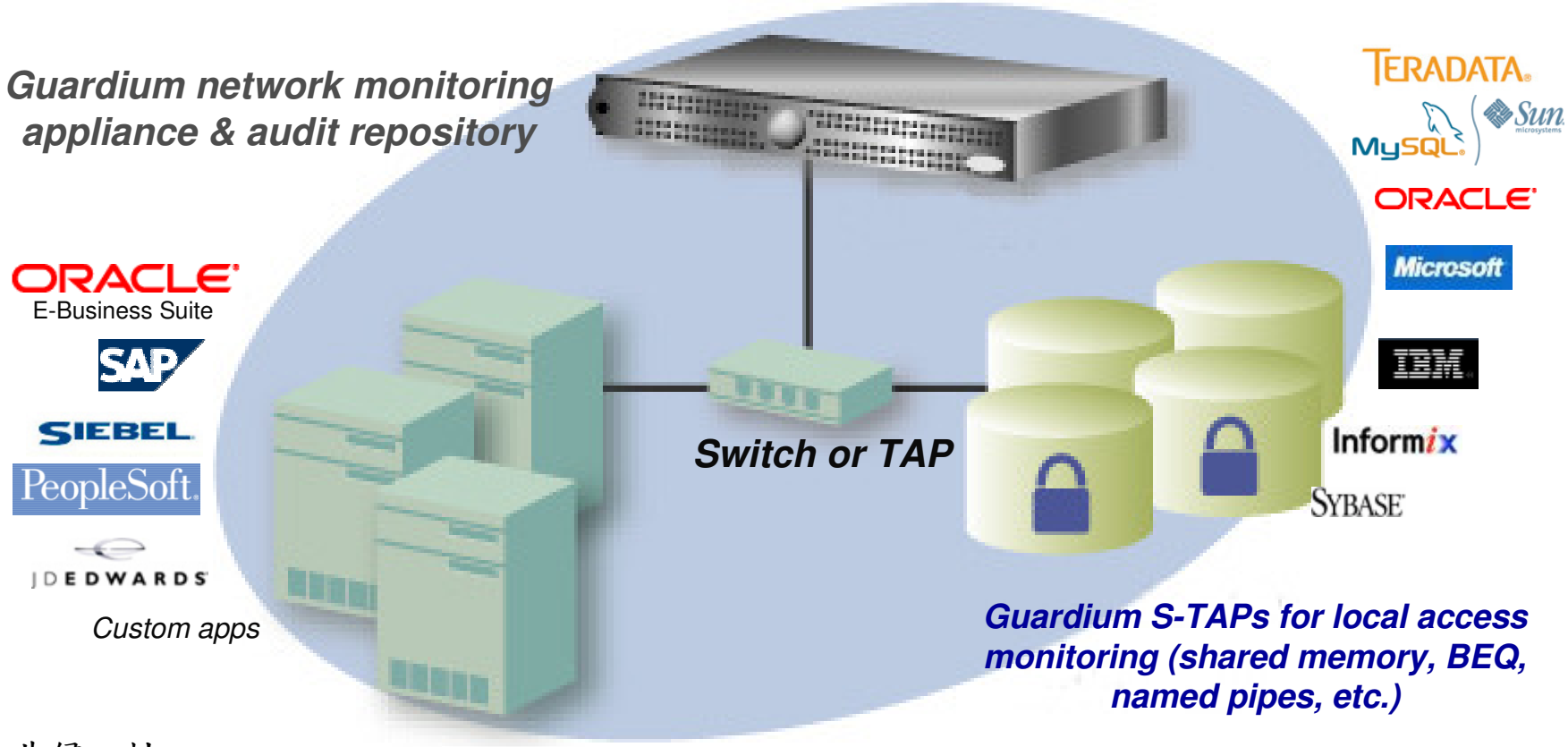






A Smarter Planet SmarterSecurity&Resilience

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

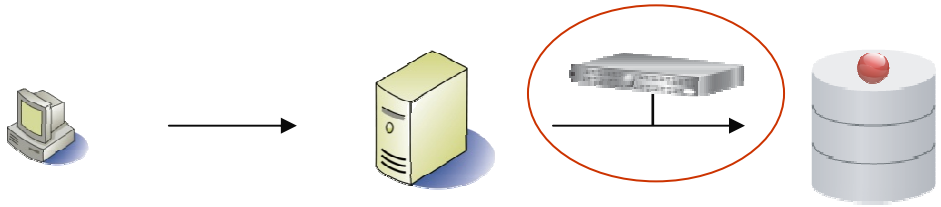


- 非侵入性
- DBMS獨立性
- 最小的系統影響
- 無需透過資料庫的日誌和稽核

- 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

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



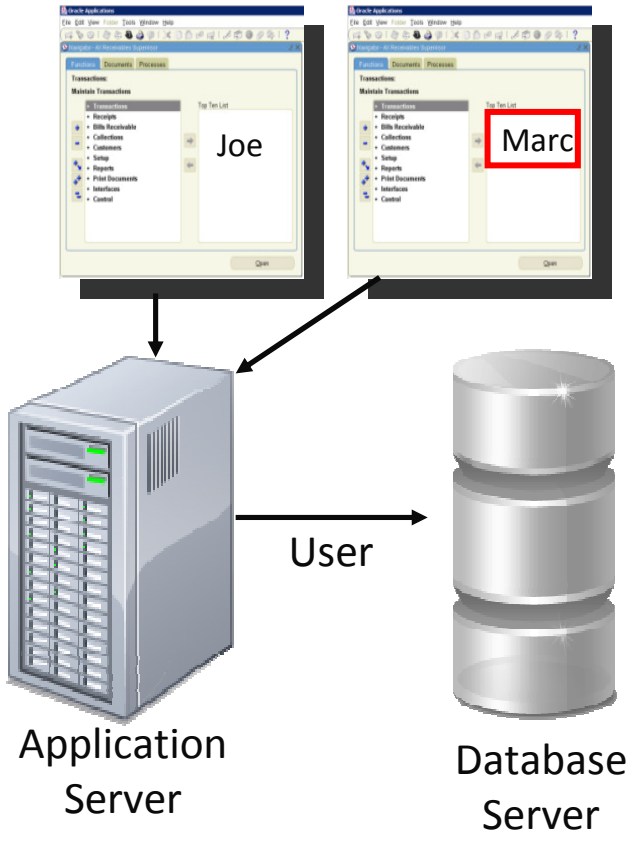
Client IP
Client host name
Domain login
Client OS
MAC
TTL
Origin
Failed logins

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

21

也可識別在應用層的詐欺行為



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

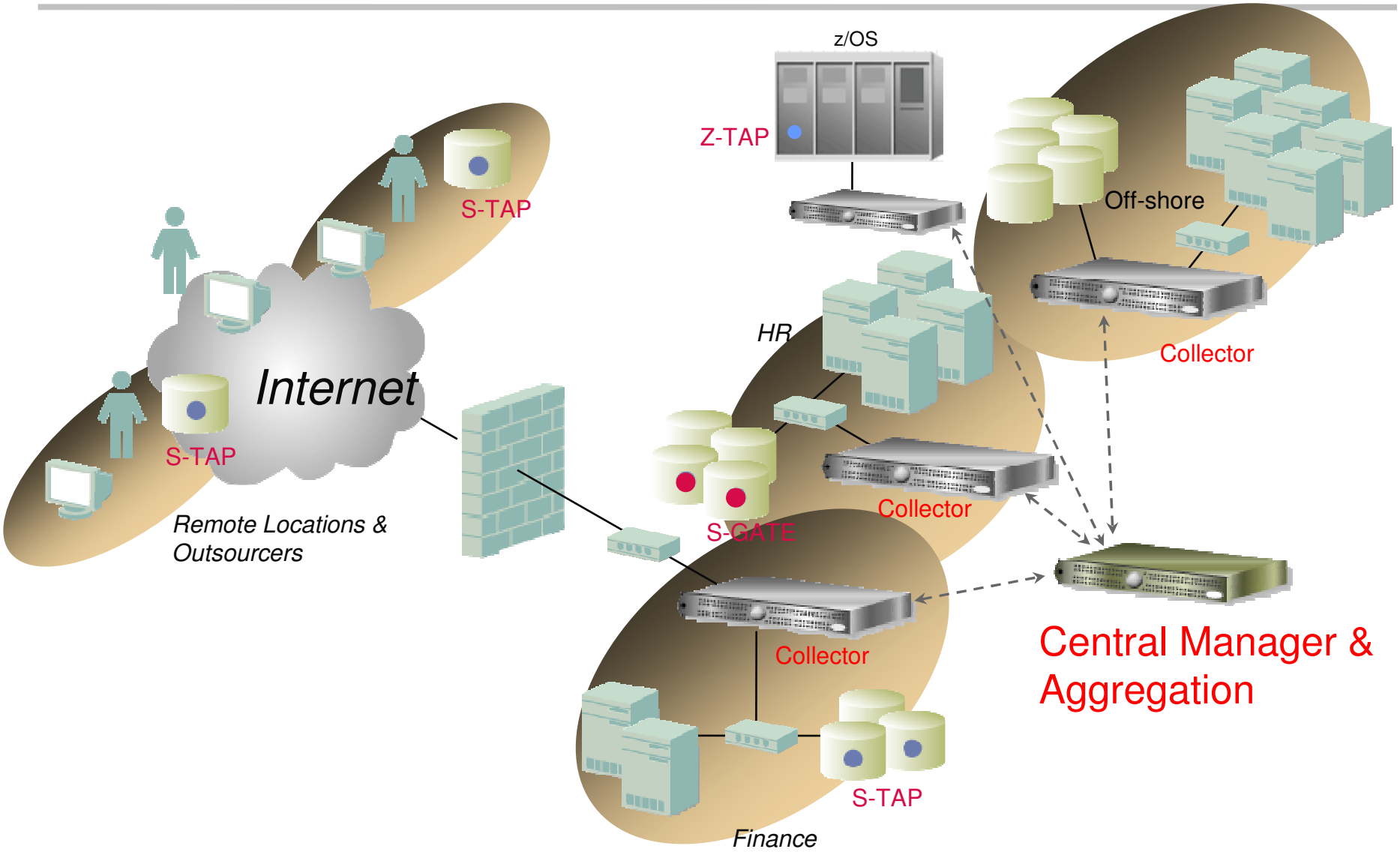
Issue:應用程式伺服器使用通用服務帳戶存取資料庫

無法驗證是誰啟動此交易行為 (connection pooling)

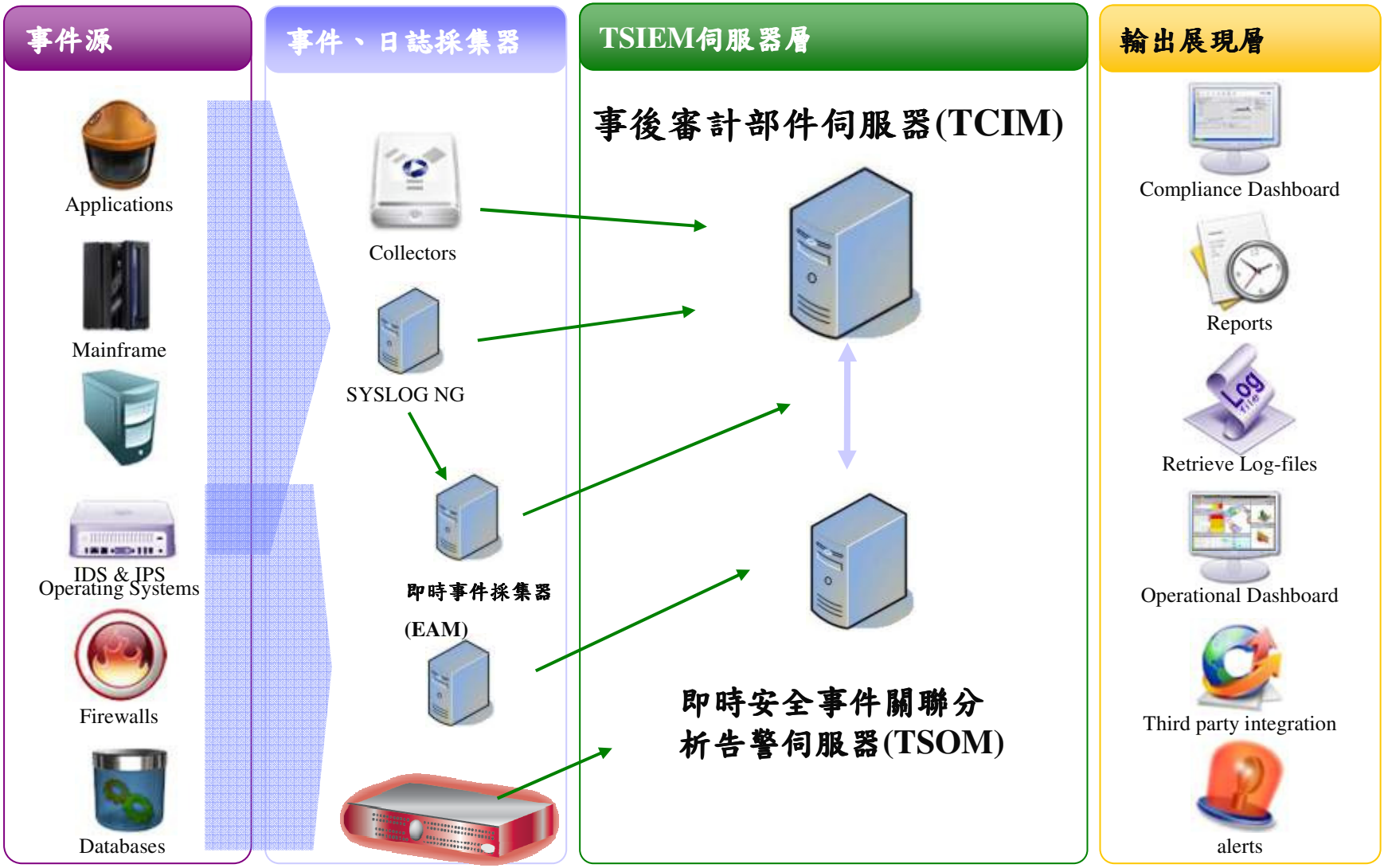
Solution: Guardium可追蹤於相關聯的應用程式使用特定的使用者ID存取SQL 指令

Out-of-the-box support for all major enterprise applications (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) and custom applications (WebSphere….)

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



IBM內部使用者行為稽核、日誌集中管理及分析、資料庫稽核與防護等方案可以與企業既有環境整合



Smarter Security and Resilience

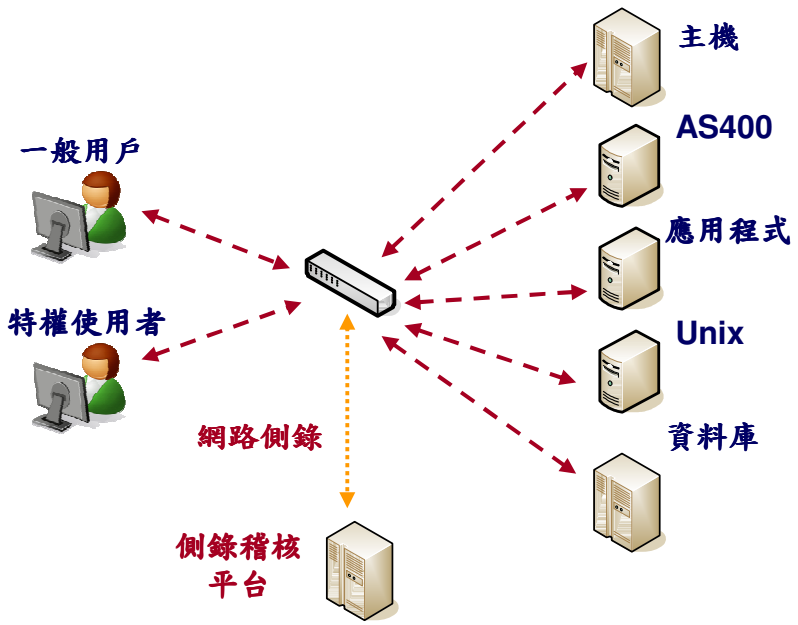
An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 作業風險與內部稽核的挑戰
- 系統架構與功能
  - 內部使用者行為稽核
  - 日誌集中管理及分析
  - 資料庫稽核與防護
- 方案應用範例
- 效益與總結

內部使用者行為稽核的應用方式：可僅簡易地監控及搜尋用戶行為

① 側錄



② 搜尋

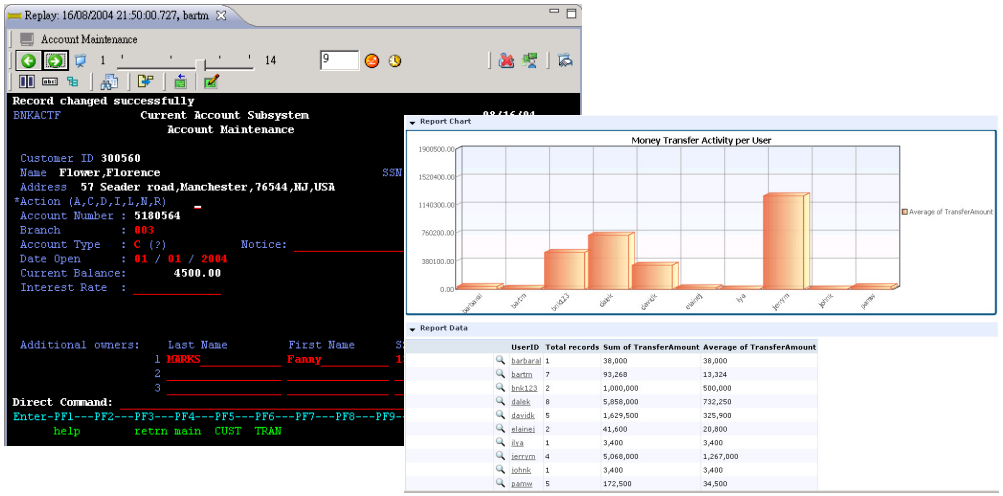
資安稽核員

用戶ID、操作頻道、時間範圍、來源與目的設備

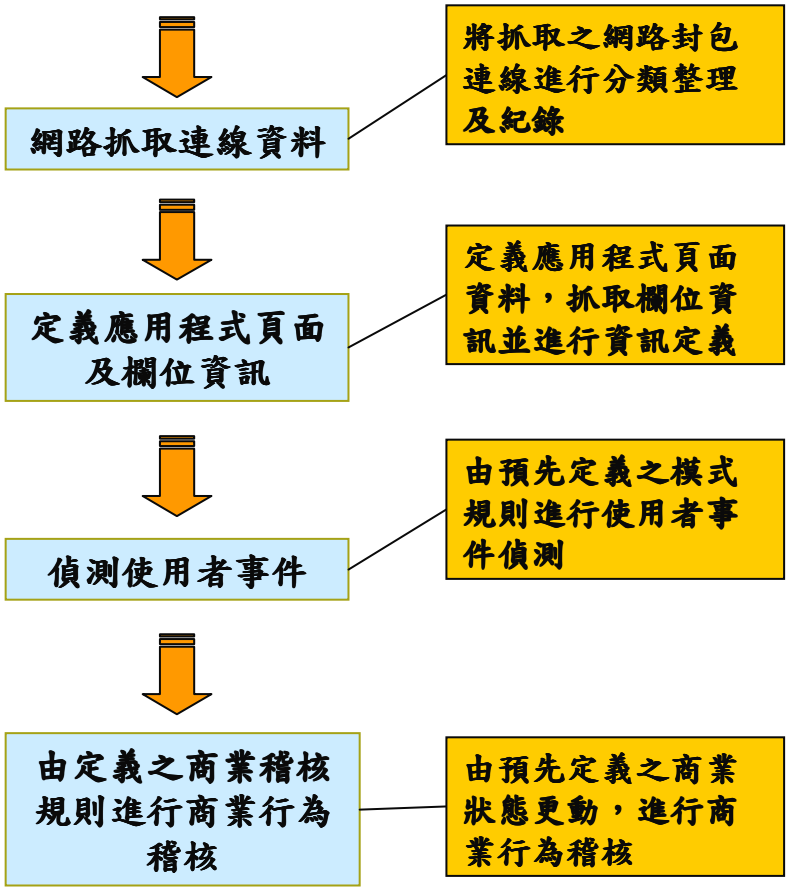
連線內之字串搜尋，正規表示式

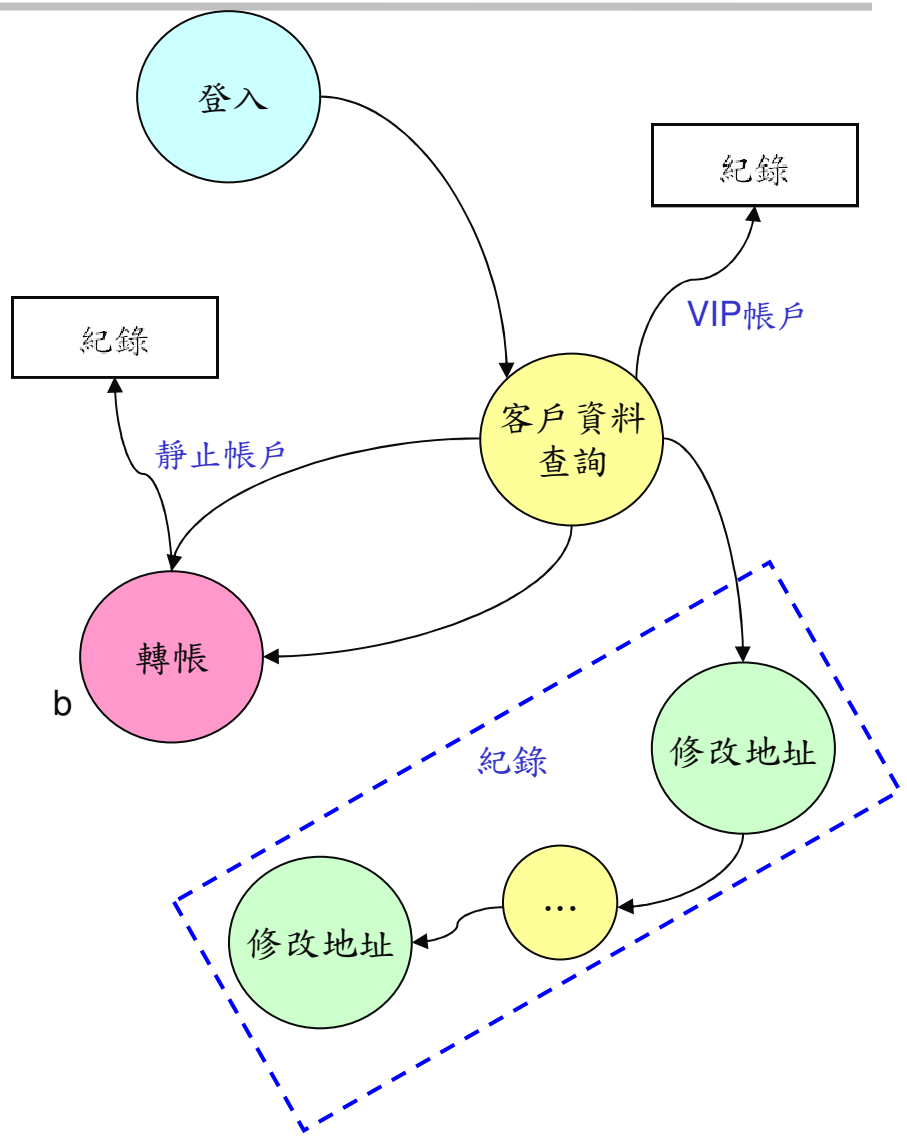
③ 用戶行為畫面或報表呈

資安稽核員



內部使用者行為稽核方案的應用方式(或亦可訂定複雜的商業規則稽核)





內部使用者行為稽核實際應用

場景1 – 檢測重要客戶資訊被存取洩漏的內部欺詐行為

企業發現可能在4月16日~23日之間，有內部員工流覽了帳號為5180774的重要客戶資訊並賣給第三方，企業要如何檢測到？

consumeraffairs.com
knowledge is power!

Countrywide Warns Millions of Data Breach

Former employee sold customer records for two years

Countrywide Financial

abc NEWS start here

Passport Security Breach on McCain, Clinton & Obama

State Department Contract Employees Fired, Another Disciplined for Looking at Passport File

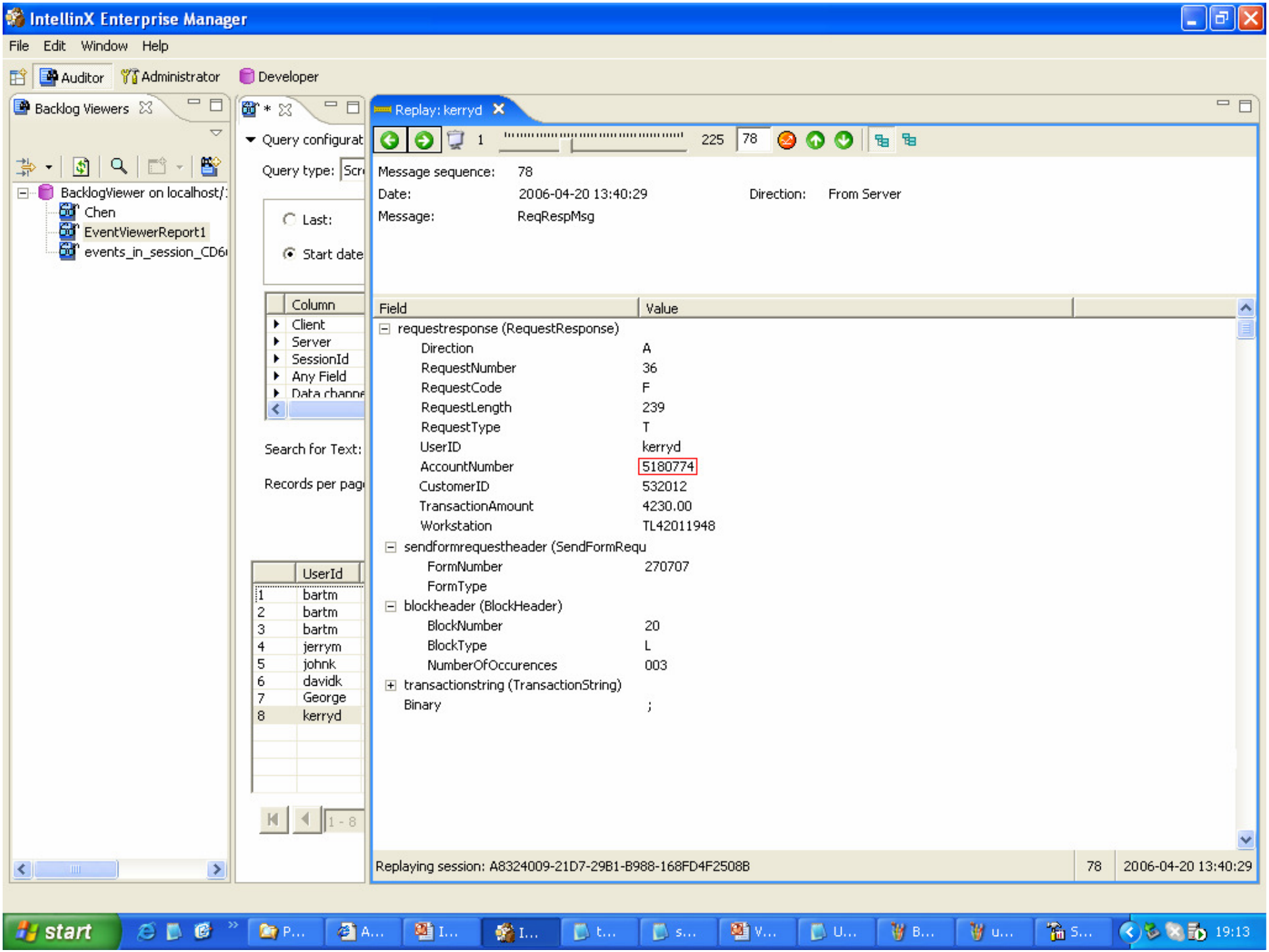
Los Angeles Times

Archive for Saturday, March 15, 2008

UCLA workers snooped in Spears' medical records

ComplianceHome
Regulatory Compliance Portal

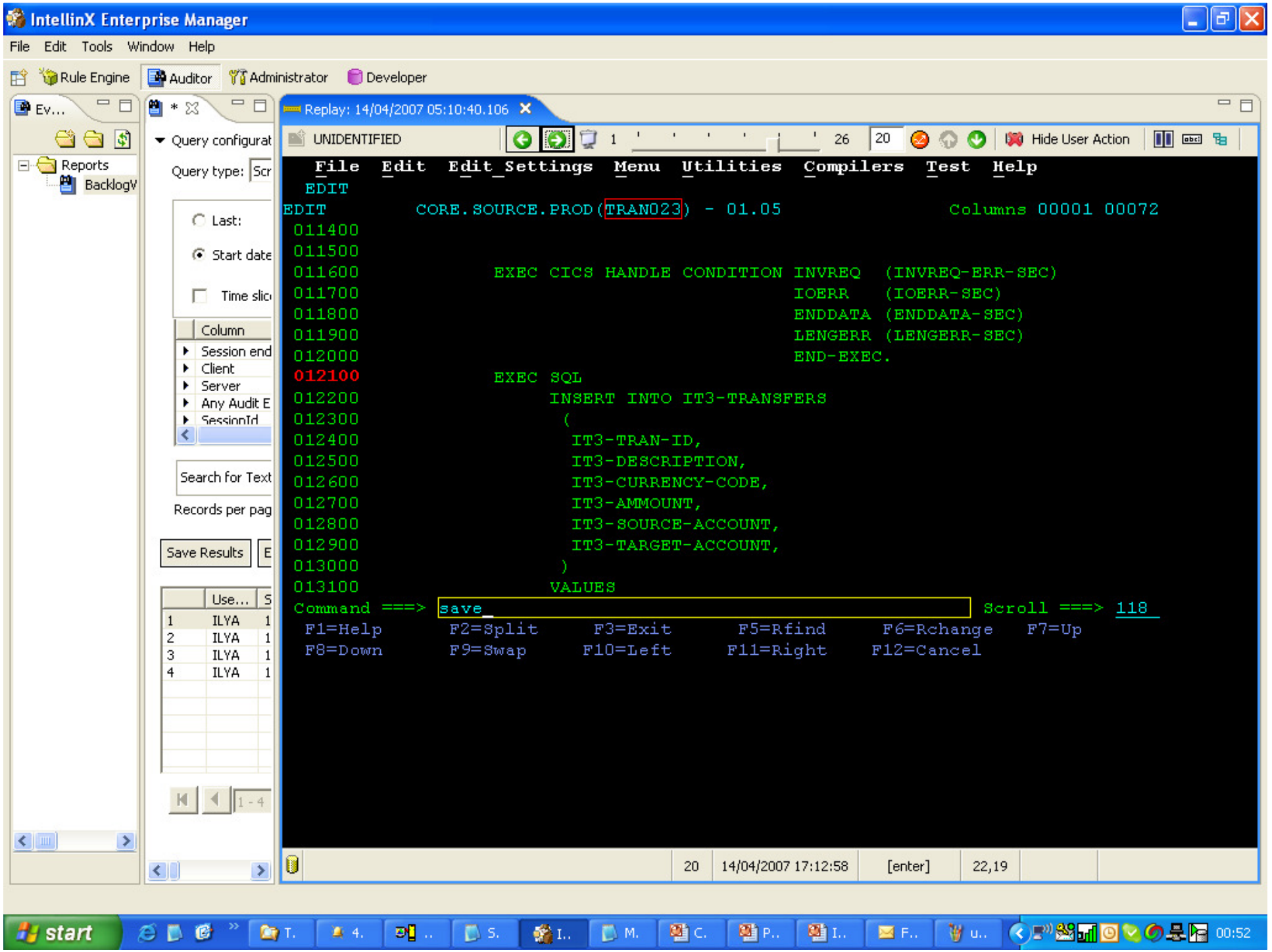
Alleged Breach of George Clooney's Health Information Leads to Suspension of 27 Staff at N.J. Medical Center


IntellinX Enterprise Manager
File Edit Window Help
Auditor
Administrator
Developer
Backlog Viewers
BacklogViewer on localhost/:
Chen
EventViewerReport1
events_in_session_CD6
Query configurat
Query type:
Last:
Start date
Column
Client
Server
SessionId
Any Field
Search for Text:
Records per pag
UserId
1 bartm
2 bartm
3 bartm
4 jerrym
5 johnk
6 davidk
7 George
8 kerryd
1 - 8
Replay: kerryd
1
225
78
Message sequence: 78
Date: 2006-04-20 13:40:29
Direction: From Server
Message: ReqRespMsg
Field
Value
requestresponse (RequestResponse)
Direction A
RequestNumber 36
RequestCode F
RequestLength 239
RequestType T
UserID kerryd
AccountNumber 5180774
CustomerID 532012
TransactionAmount 4230.00
Workstation TL42011948
sendformrequestheader (SendFormRequ
FormNumber 270707
FormType
blockheader (BlockHeader)
BlockNumber 20
BlockType L
NumberOfOccurences 003
transactionstring (TransactionString)
Binary ;
Replaying session: A8324009-21D7-29B1-B988-168FD4F2508B
78
2006-04-20 13:40:29
start
19:13

內部使用者行為稽核實際應用

場景2 – 檢測重要程式碼被惡意員工修改的內部欺詐行為

企業發現於指定日期區間中，編號為TRAN023的主機程式有一些不當的資料庫存取行為，但經由Review程式碼看不出原因到底為何。企業要如何能夠檢測到並避免此類行為？


IntellinX Enterprise Manager
File Edit Tools Window Help
Rule Engine
Auditor
Administrator
Developer
Reports
BacklogV
Query configurat
Query type:
Last:
Start date
Time slic
Column
Session end
Client
Server
Any Audit E
SessionId
Search for Text
Records per pag
Save Results
Use...
1 ILYA 1
2 ILYA 1
3 ILYA 1
4 ILYA 1
1 - 4
Replay: 14/04/2007 05:10:40.106
UNIDENTIFIED
Hide User Action
File Edit Edit_Settings Menu Utilities Compilers Test Help
EDIT
EDIT CORE.SOURCE.PROD(TRAN023) - 01.05 Columns 00001 00072
011400
011500
011600 EXEC CICS HANDLE CONDITION INVREQ (INVREQ-ERR-SEC)
011700 IOERR (IOERR-SEC)
011800 ENDDATA (ENDDATA-SEC)
011900 LENGERR (LENGERR-SEC)
012000 END-EXEC.
012100 EXEC SQL
012200 INSERT INTO IT3-TRANSFERS
012300 (
012400 IT3-TRAN-ID,
012500 IT3-DESCRIPTION,
012600 IT3-CURRENCY-CODE,
012700 IT3-AMMOUNT,
012800 IT3-SOURCE-ACCOUNT,
012900 IT3-TARGET-ACCOUNT,
013000)
013100 VALUES
Command ===> save
Scroll ===> 118
F1=Help F2=Split F3=Exit F5=Rfind F6=Rchange F7=Up
F8=Down F9=Swap F10=Left F11=Right F12=Cancel
20 14/04/2007 17:12:58 [enter] 22,19
start
00:52

內部使用者行為稽核方案可應用於金融行業之商業規則範例

1. 單一使用者或終端機的異常查詢行為

- 針對客戶資料進行過度且異常之查詢
- 針對VIP客戶或是靜止客戶進行查詢

2. 須警示的異常交易行為

- 設定相同之帳戶地址至多個客戶帳戶
- 設定相同之約定轉帳帳戶至多個客戶帳戶
- 超過某訂定額度之交易
- 修改客戶帳戶地址資料，之後再將其改回來
- 於客戶帳戶內新增約定轉帳帳戶，後續再修改回來

3. 非上班時間所進行之查詢或異動交易

內部使用者行為稽核方案可應用於IT管理面之商業規則範例

1. 更動管理控管

- 由IT組織內之使用者，於production環境內利用特定工具進行查詢或修改
- 於production環境內進行程式安裝、修改或組態更動

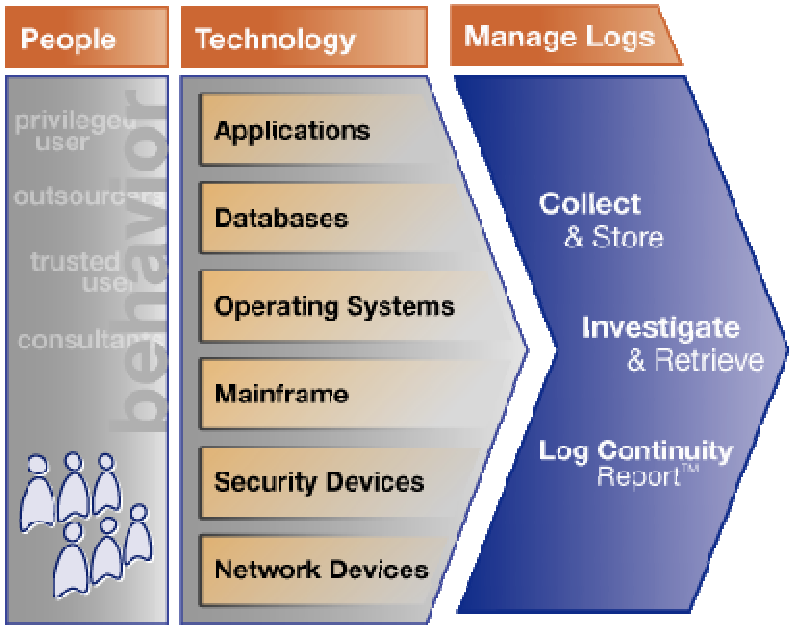
2. 異常行為監控

- 於production環境內安裝程式，執行後，將程式刪除
- 於非上班時間，由IT網段利用業務單位之user-id登入
- 採用同一使用者帳戶於多台終端機登入，或於單台終端機有多個使用者帳戶登入

3. 特權管理員稽核

- 特權管理員登入後行為紀錄
- 一般使用者利用指令轉換身份為特權管理員

日誌集中管理及分析的第一步：抓取日誌 (Capture)



Capture

功能：

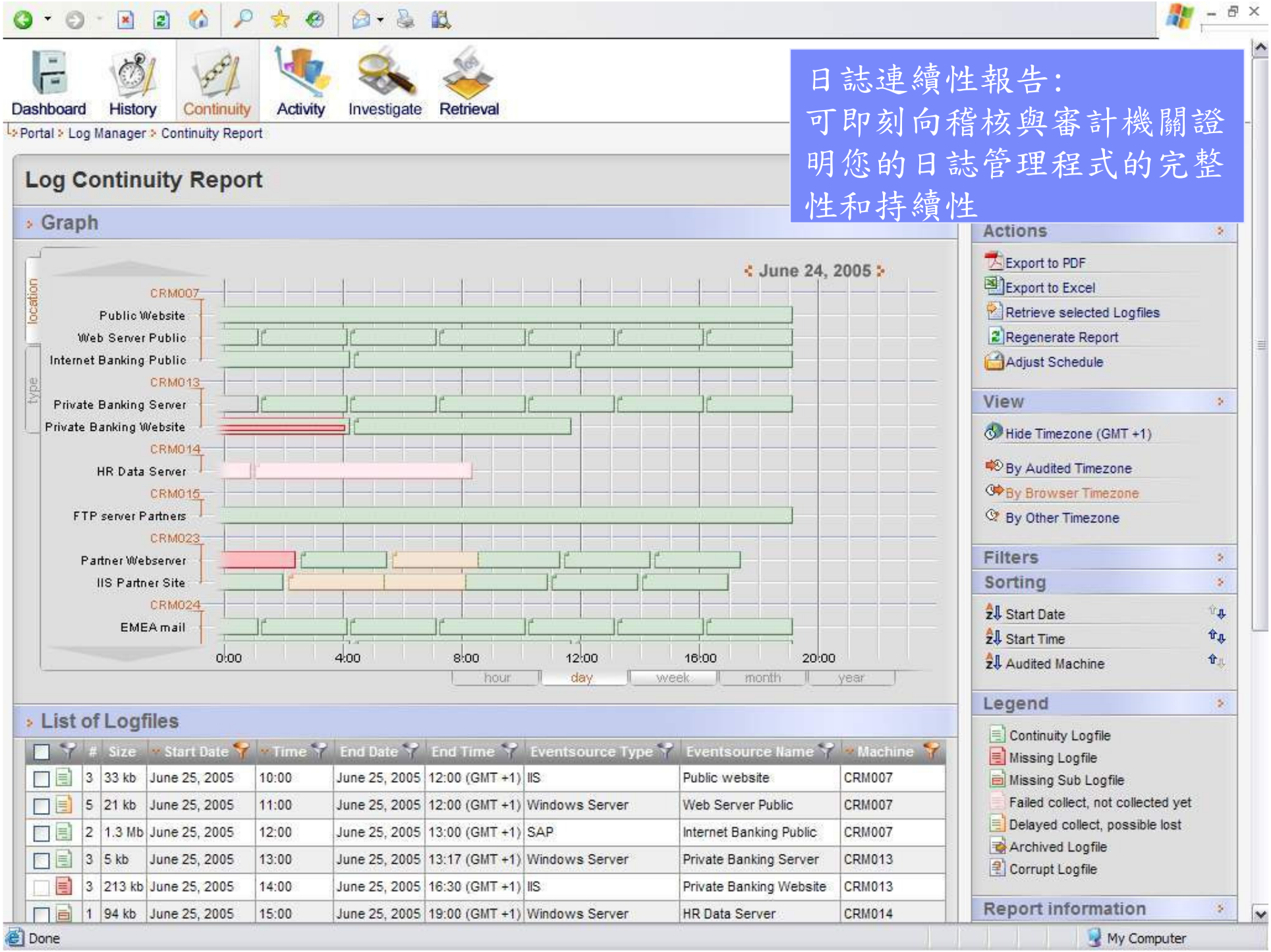
- 從任何平台上安全可靠地捕獲日誌
- 全面支援原始日誌收集和保存
- 將日誌保存在經過壓縮的高效存儲庫中
- 在需要時可以存取原始資料
- 提供所有原始日誌中查找關鍵資料
- 通過報告證明對日誌進行了全面收集

成效：

集中的自動收集日誌可降低成本

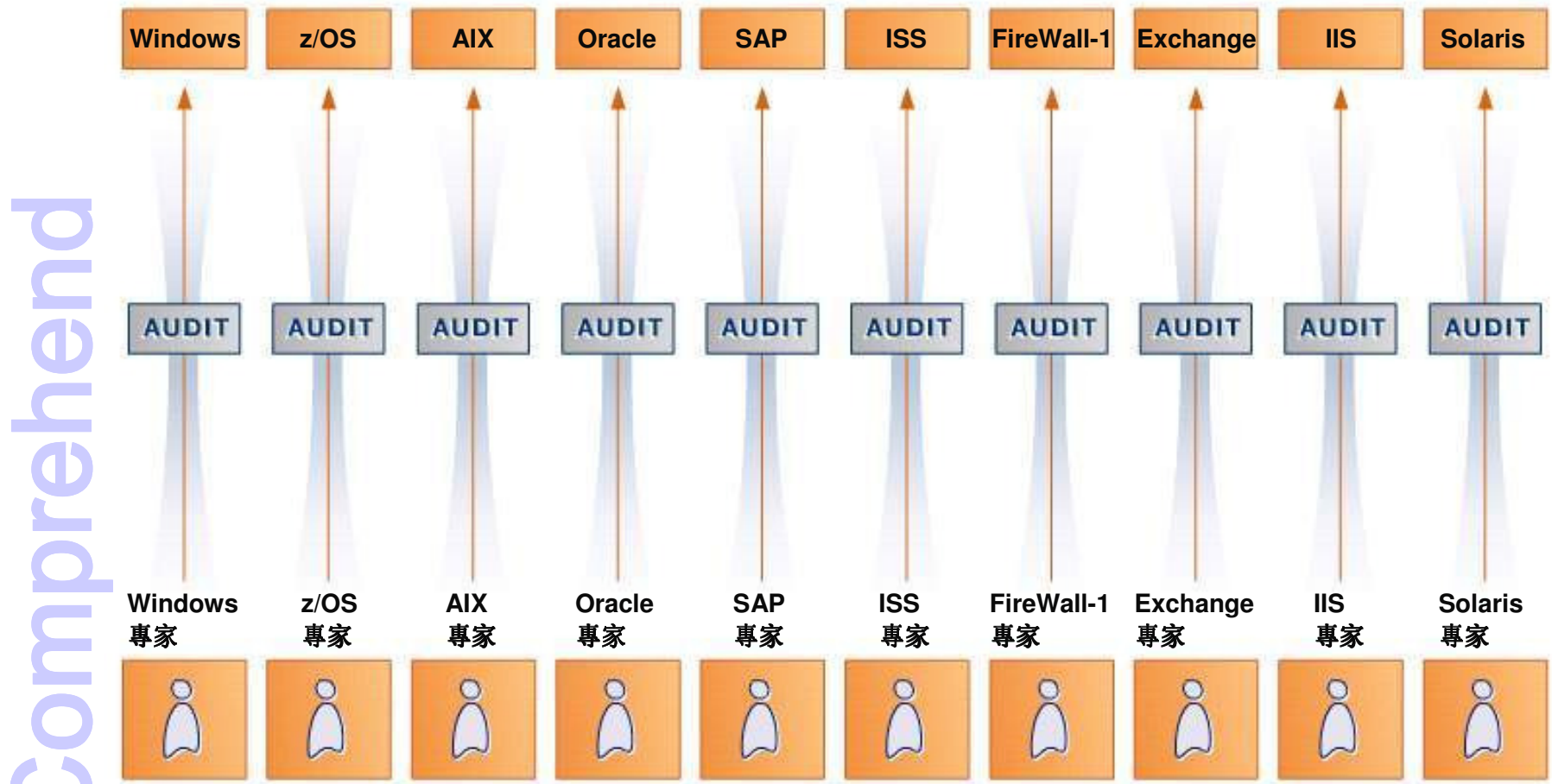
隨時應對 “審計”！

實施時間：即插即用

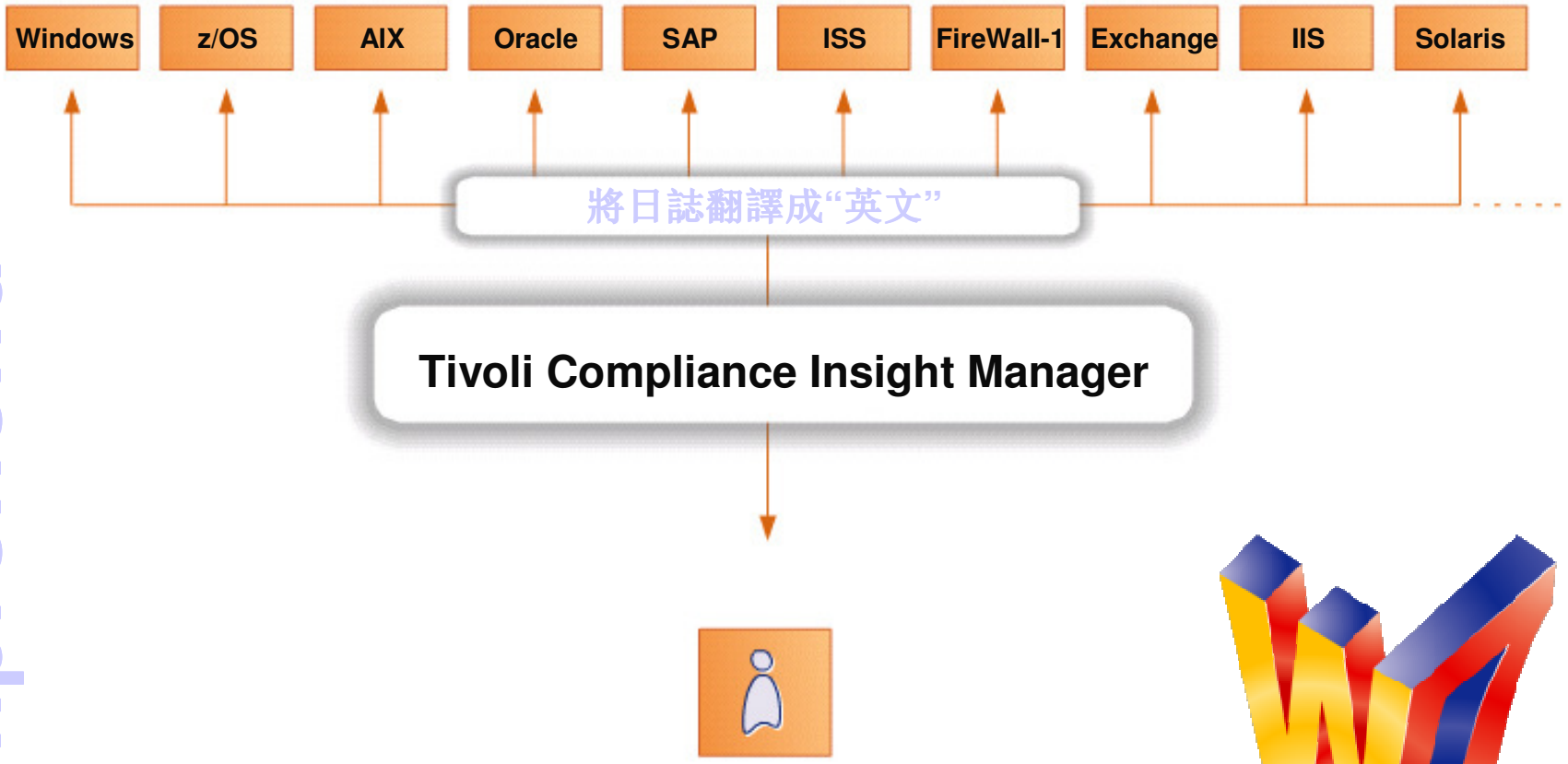


日誌連續性報告：
可即刻向稽核與審計機關證明您的日誌管理程式的完整性和持續性

日誌收集後的工作是翻譯



通過自動翻譯實現日誌標準化



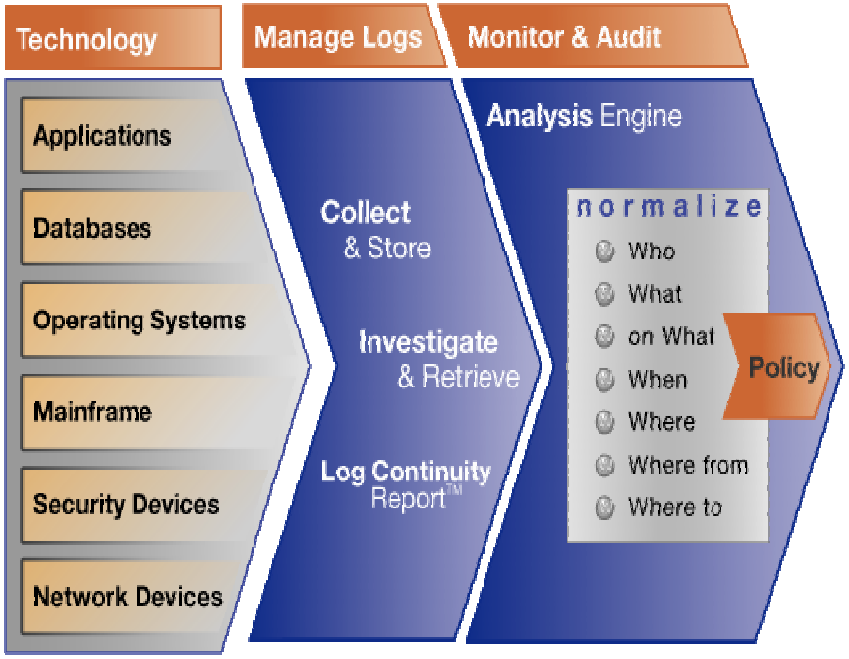
Comprehend

***Who** did **What** type of action **on What**?*

***When** did he do it and **Where**, **From Where** and **Where To**?*

日誌集中管理及分析的第二步：關聯與理解 (Comprehend)

Comprehend



功能：

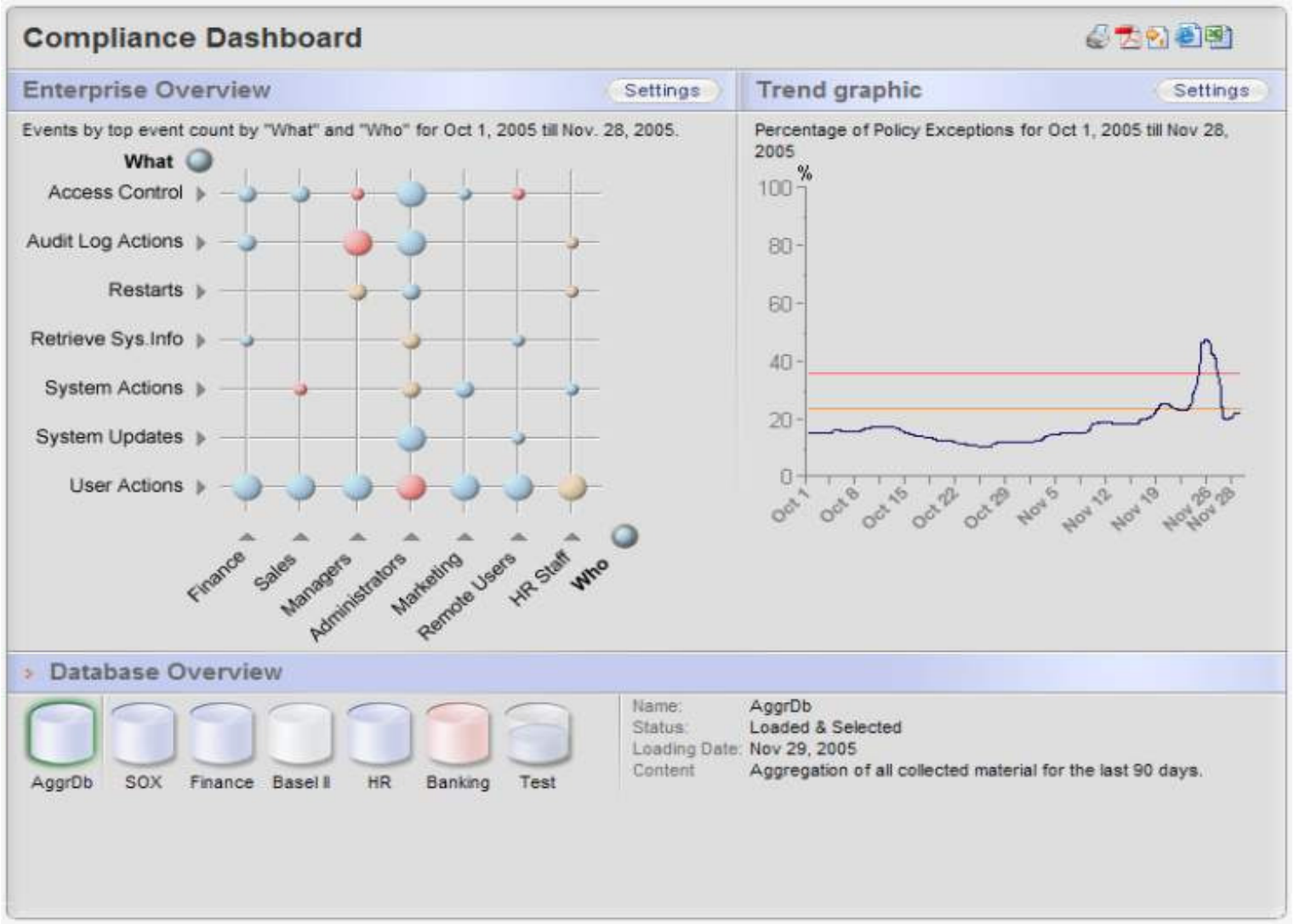
- 日誌的W7 標準化
- 將日誌專案與基準制度進行比較，從而判定違規行為，違規級別

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

現成的日誌標準化工具！

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



日誌集中管理及分析的第三步：瞭解與調查 (Communicate)

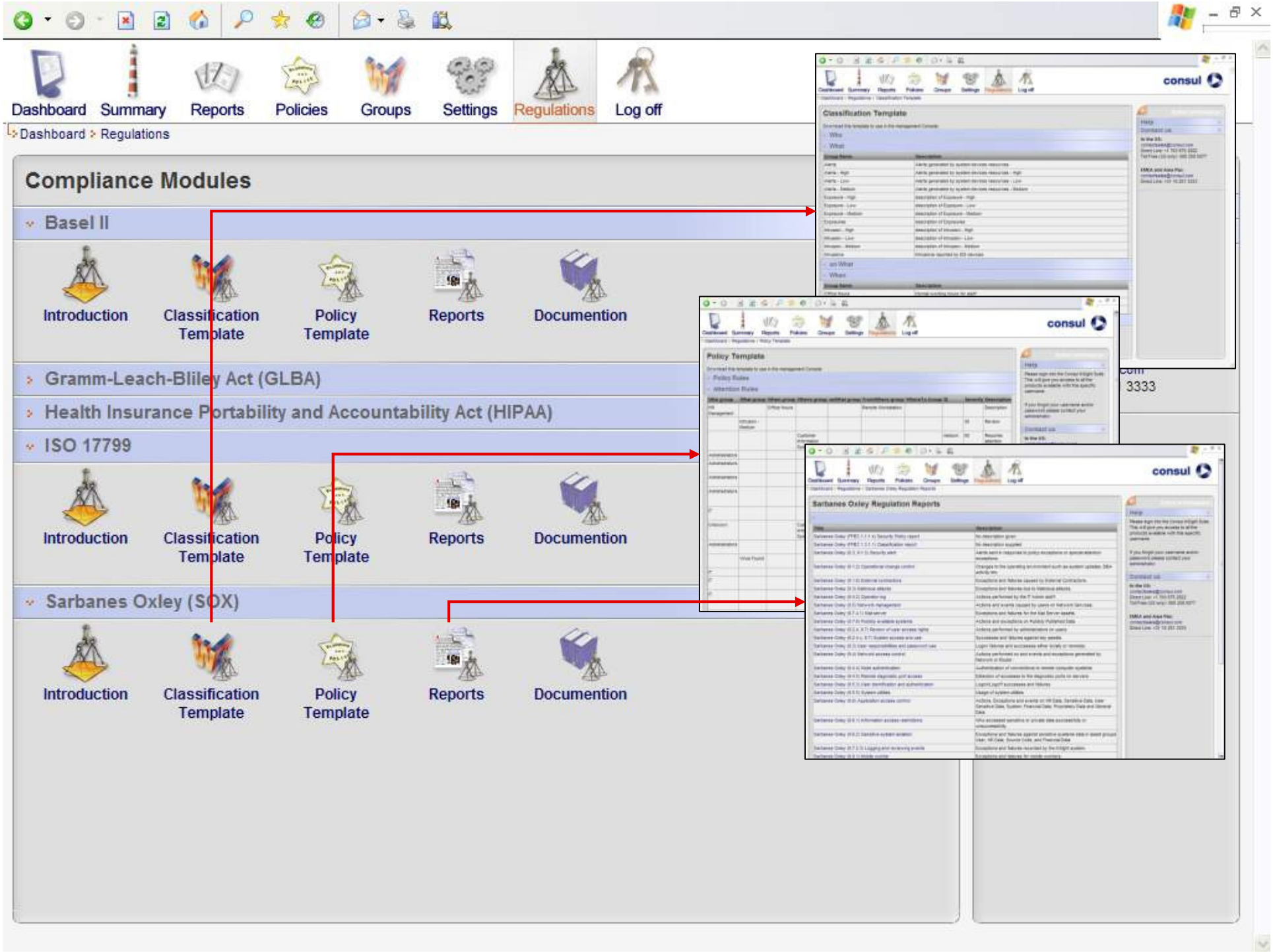
Communicate

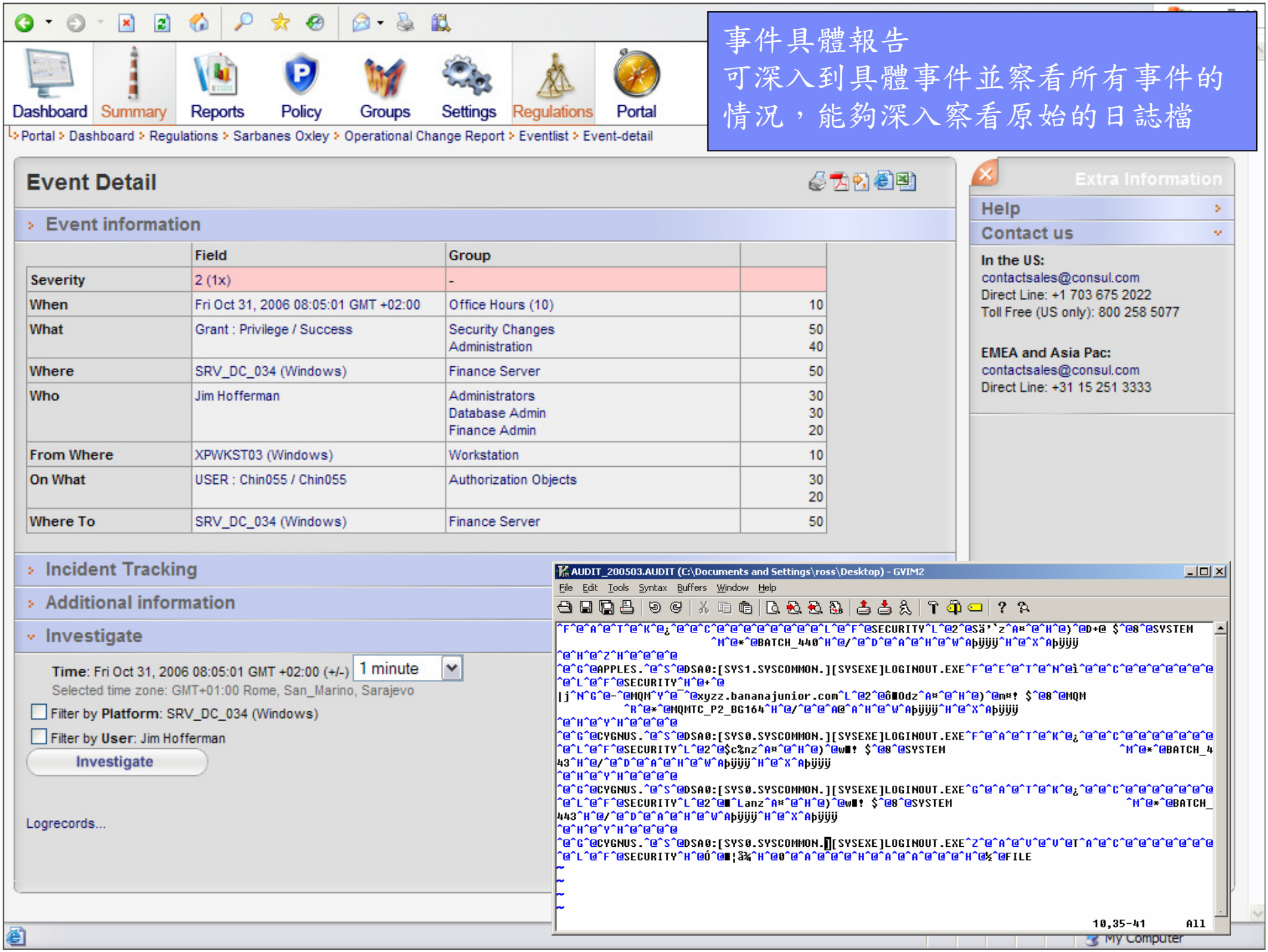
功能：

- 幾百個報告
- 制度遵從模組
- 重要告警事件
- 定制報告
- 原始日誌調查工具

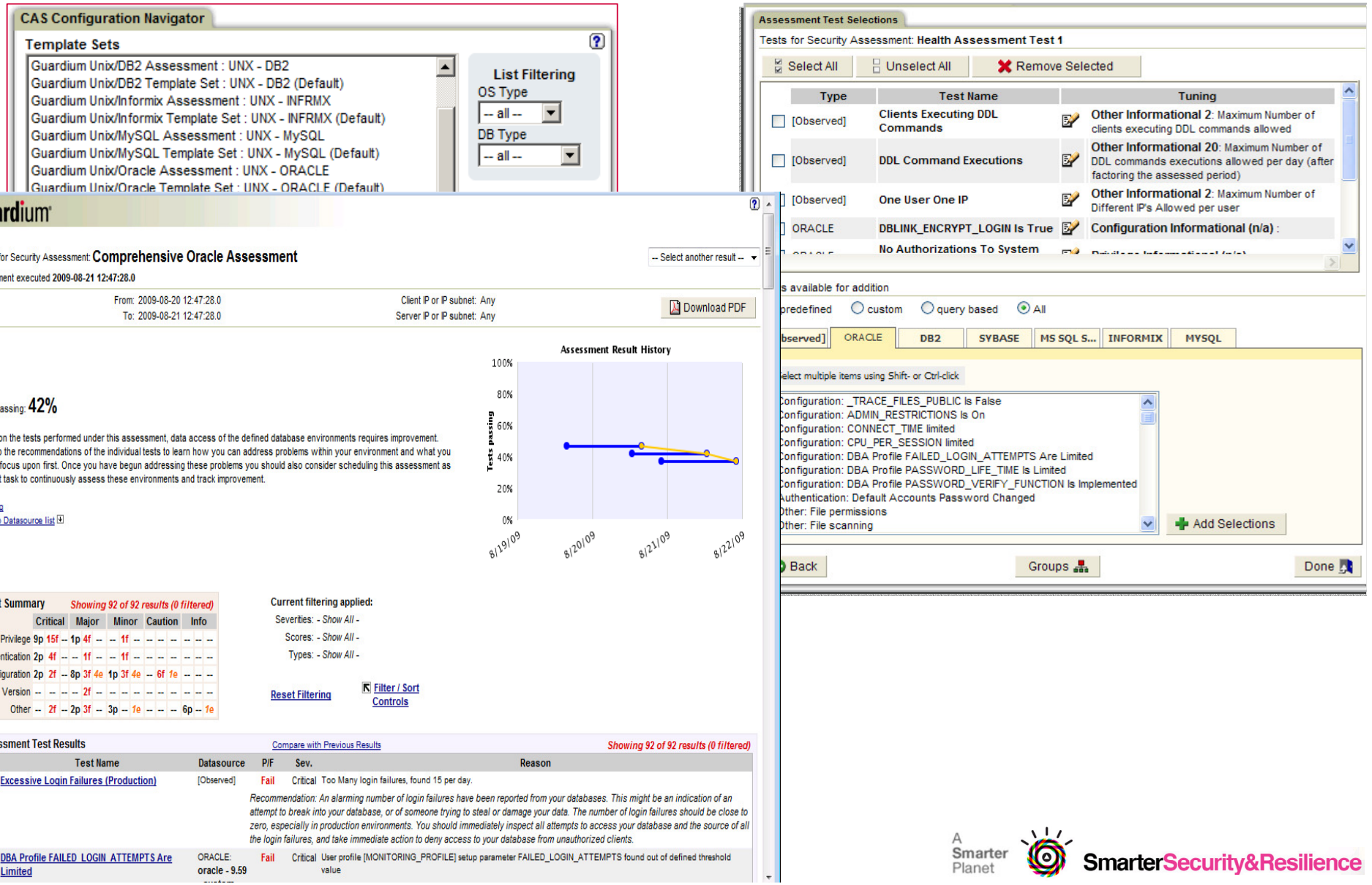
成效：

- 幫助審計公司省時省力
- 即時報告，節省時間
- 降低內部威脅風險：
  - 資訊保護
  - 變化控制
  - 用戶管理


Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard > Regulations
Compliance Modules
Basel II
Introduction
Classification Template
Policy Template
Reports
Documention
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
ISO 17799
Introduction
Classification Template
Policy Template
Reports
Documention
Sarbanes Oxley (SOX)
Introduction
Classification Template
Policy Template
Reports
Documention
consul
Classification Template
consul
Policy Template
consul
Sarbanes Oxley Regulation Reports

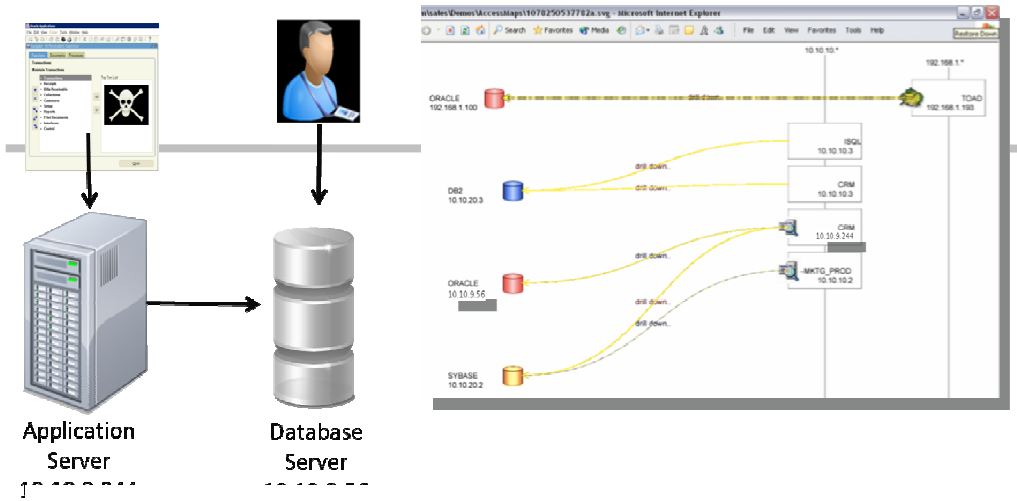

事件具體報告
可深入到具體事件並察看所有事件的情況，能夠深入察看原始的日誌檔
Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-detail
Event Detail
Event information
Field
Group
Severity
2 (1x)
-
When
Fri Oct 31, 2006 08:05:01 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
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...
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
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
10,35-41 All
My Computer

資料庫稽核與防護方案支援各種事先定義的弱點評估測試

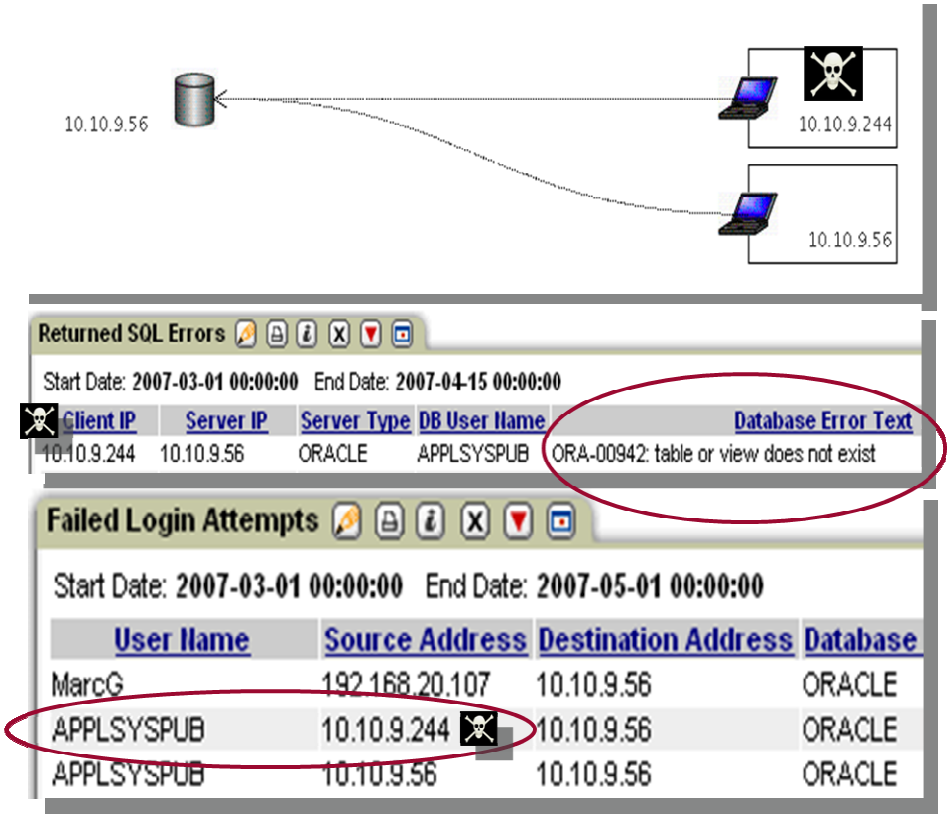


A Smarter Planet

SmarterSecurity&Resilience



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

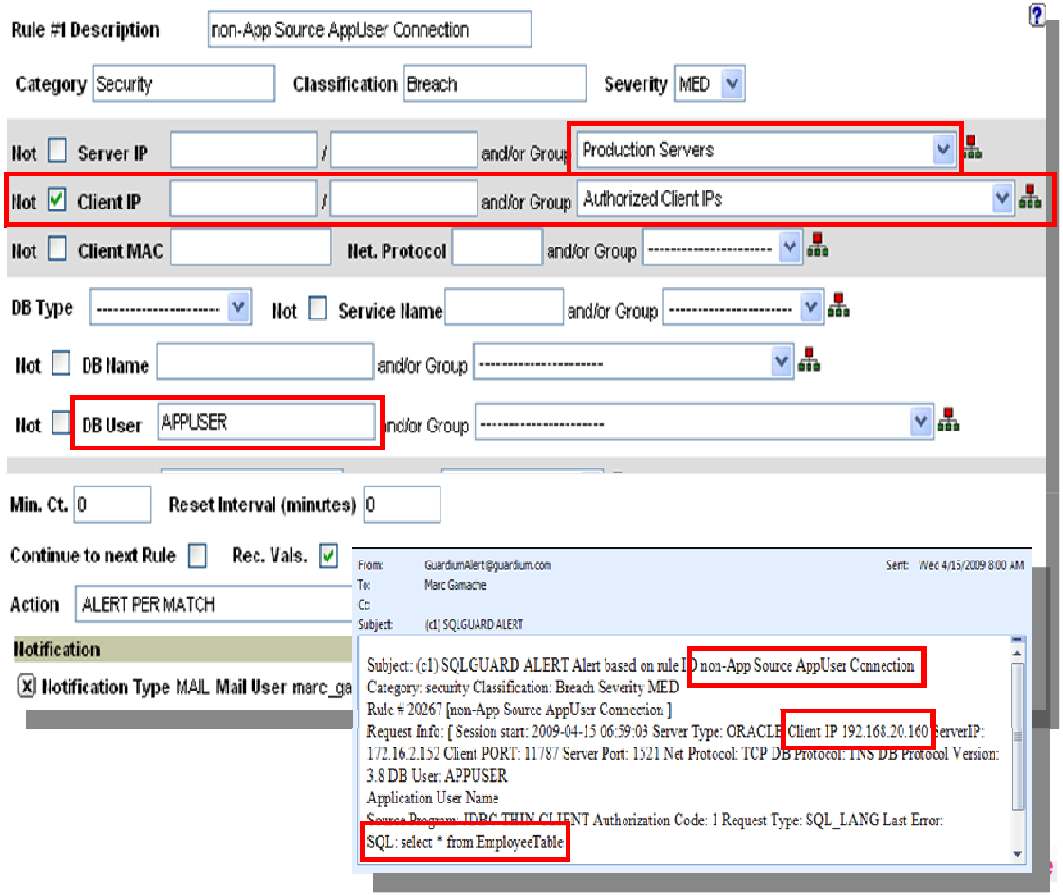


為什麼正式系統中會有應用系統存取資料庫，卻發生找不到此資料表呢？

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？



雖然式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

谁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

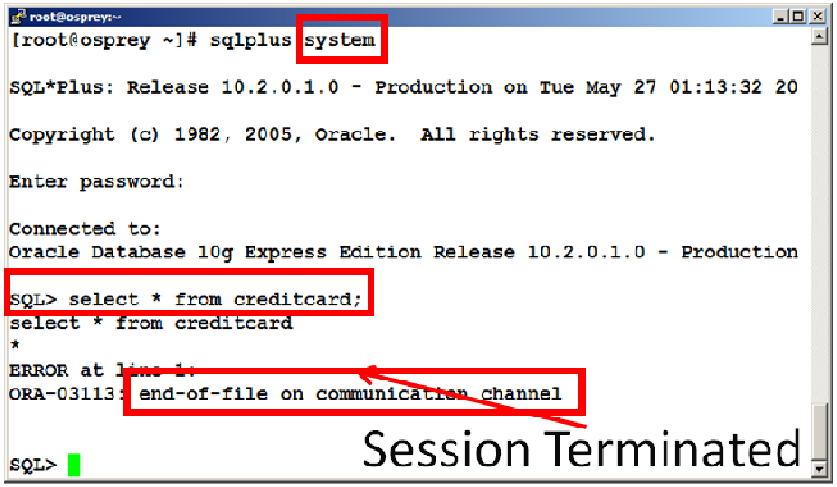
DB User Name	Sql
SYSTEM	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

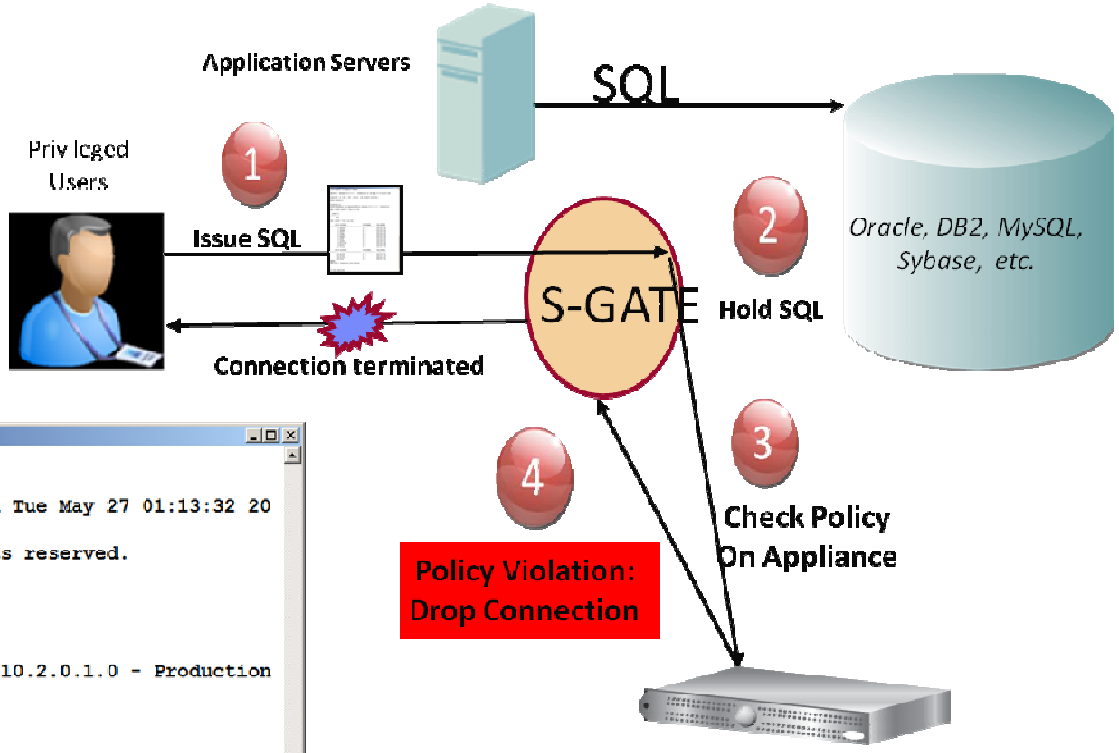
DB User Name	ShellAcct	Sql
SYSTEM	ORACLE	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

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

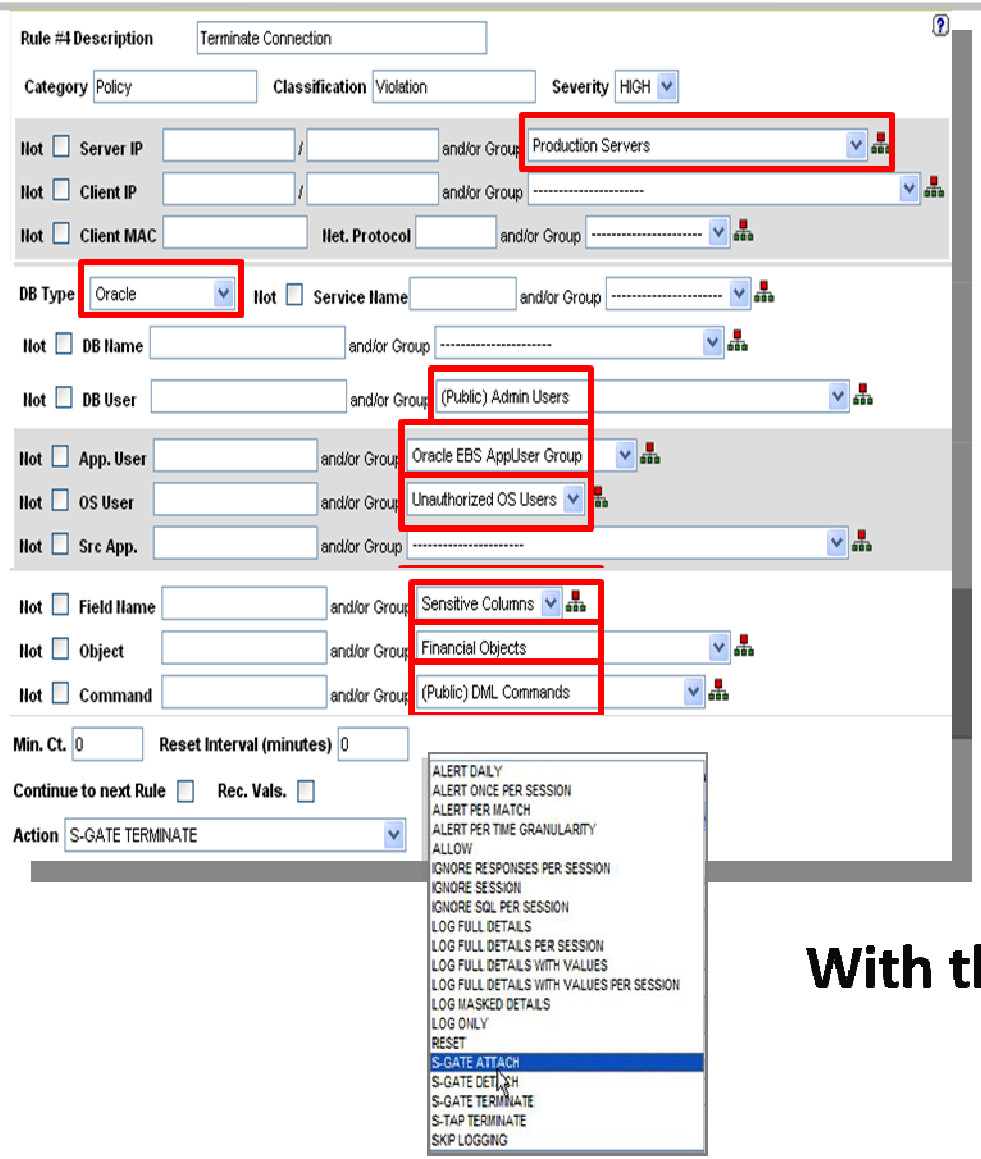
資料庫稽核與防護方案也能作及時阻斷

"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

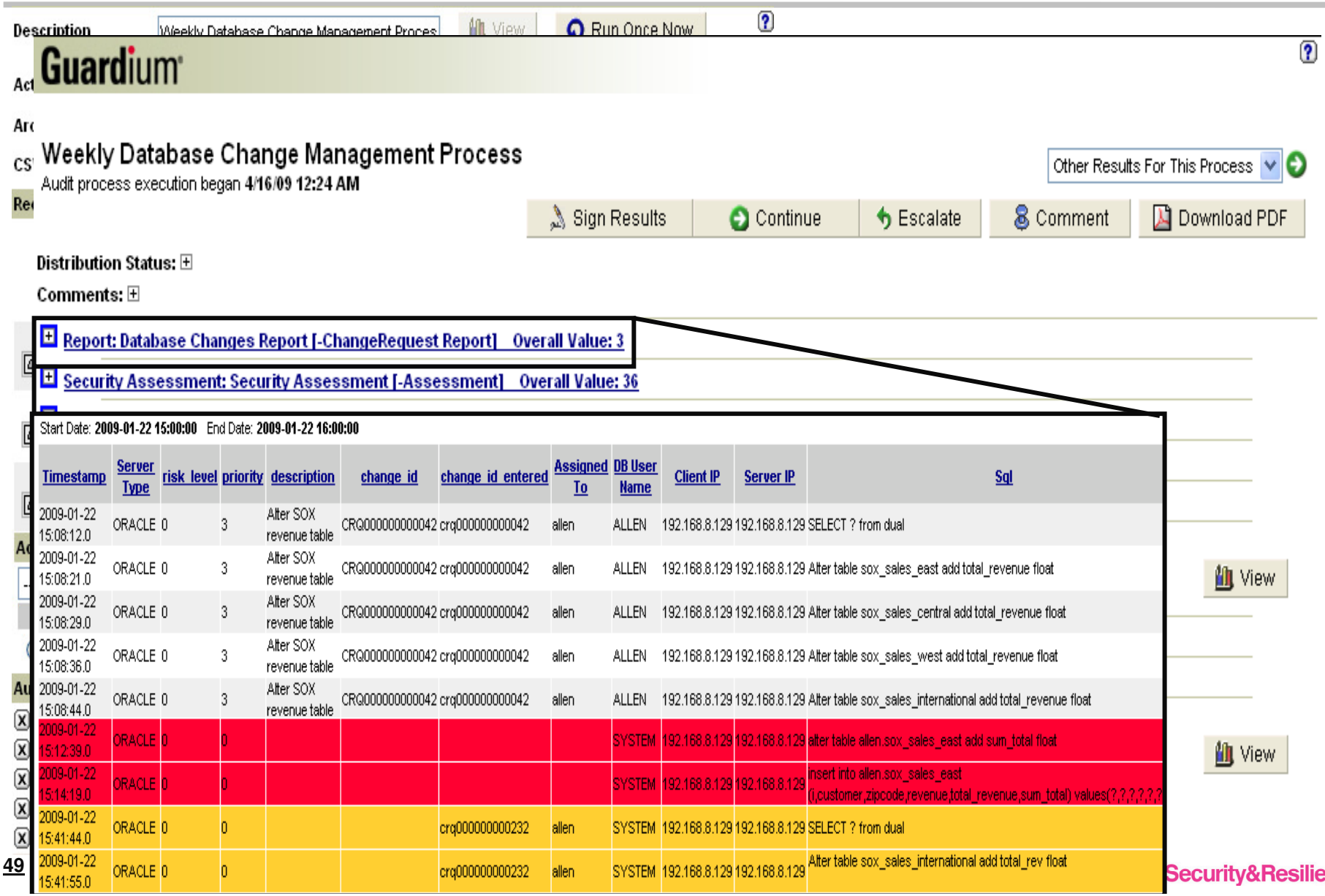
Which Databases

Which Users

Which Fields
Which Tables
Which SQL Commands

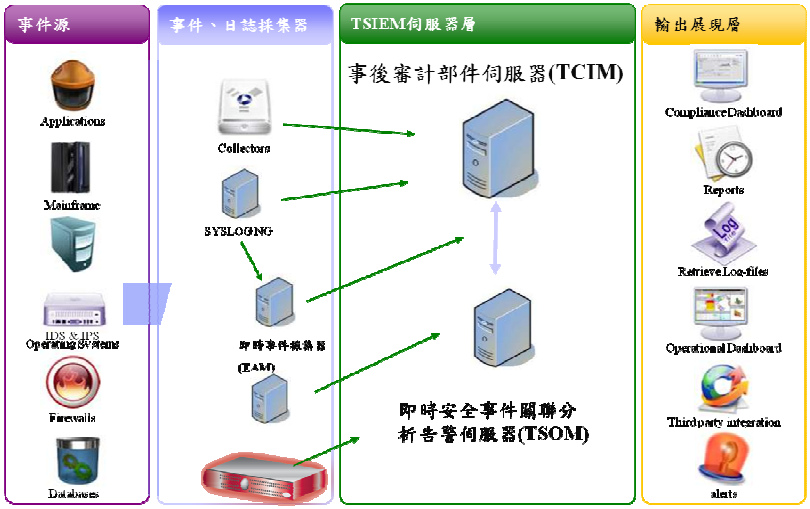
With the ability to terminate traffic!

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



Timestamp	Server Type	risk level	priority	description	change id	change id entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

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



Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 作業風險與內部稽核的挑戰
- 系統架構與功能
  - 內部使用者行為稽核
  - 日誌集中管理及分析
  - 資料庫稽核與防護
- 方案應用範例
- 效益與總結

IBM的「資料外洩分析與處理」方案從內部使用者行為稽核、日誌集中管理及分析、資料庫稽核與防護等各方面帶給客戶完整的資料保護

- **安全管理能力提升** - 加強資料中心維運安全管理的能力，為資料中心系統安全維運提供保障。
- **不影響系統、網路架構** - 不佔用原本的系統資源開銷，不影響交易回應時間，針對日常業務運行不存在任何實施風險。
- **支援跨平臺交易查詢功能** - 可以查詢到交易跨平臺的完整交易流程。例如交易處理最初從IBM主機下開始，中間經過RS/6000或AS/400平臺的client-server應用處理，最終結束于web應用下。
- **完整的操作稽核記錄** - 7x24記錄所有的用戶操作，包括update操作和一般系統日誌裏不記錄的read操作和how操作，為安全管理人員提供了便捷的用戶操作稽核和監控功能，更為企業在短期內遵從法規、滿足外稽要求等提供了技術手段。
- **按照企業需求定義的稽核規則** - 可以按照企業的要求定義操作稽核規則，對各類失誤操作，違規操作和惡意操作等事件提供即時告警，幫助企業進行即時分析並及時採取措施，還可以為事後取證調查等提供證據。

- 確保企業資料的私密與完整，強化變更與存取控制、支援各種不同資料庫及物件
- 增加作業效率，自動化且集中化內部控制
- 真正能找到資料存取人，並採取保護措施
- 防止特許人員與非授權人的破壞，證明DBA的清白
- 不是只有監控與稽核，還可以及時阻斷
- 整合式的安控與資料保護儀表板及警示通知系統
- 端到端完整的事件收集與關連分析
- 按人員角色和敏感系統設定安全稽核策略，線上顯示可疑的安全事故
- 跨平臺的安全審計日誌集中歸檔，滿足對長期的稽核要求
- 100多種安全合規報告，包括依據SOX、BASELII、PCI、ISO17799/27001等生成的許可權用戶活動行為報告

內部使用者行為稽核參考客戶

Banking & Finance

GE Money
UniCredit Bank
US Bank
Raiffeisen BANK
EQUIFAX
中国农业银行 AGRICULTURAL BANK OF CHINA
TCF
bankinter
NEDBANK
לאומי leumi
SEC SECSERVIZI
Inter-Európa Bank Rt.
VOLKSBANK Hungary A BIZALOM ÖSSZEKÖT.
BancaStato BANCA DELLO STATO DEL CANTONE TICINO
BANCO J. SAFRA
משלנבת ישראכרט
ISRAEL DISCOUNT BANK
K&H

Insurance

UNIQA
AVIVA
HAREL Insurance & Finance
מגדל
cial Insurance
Groupama

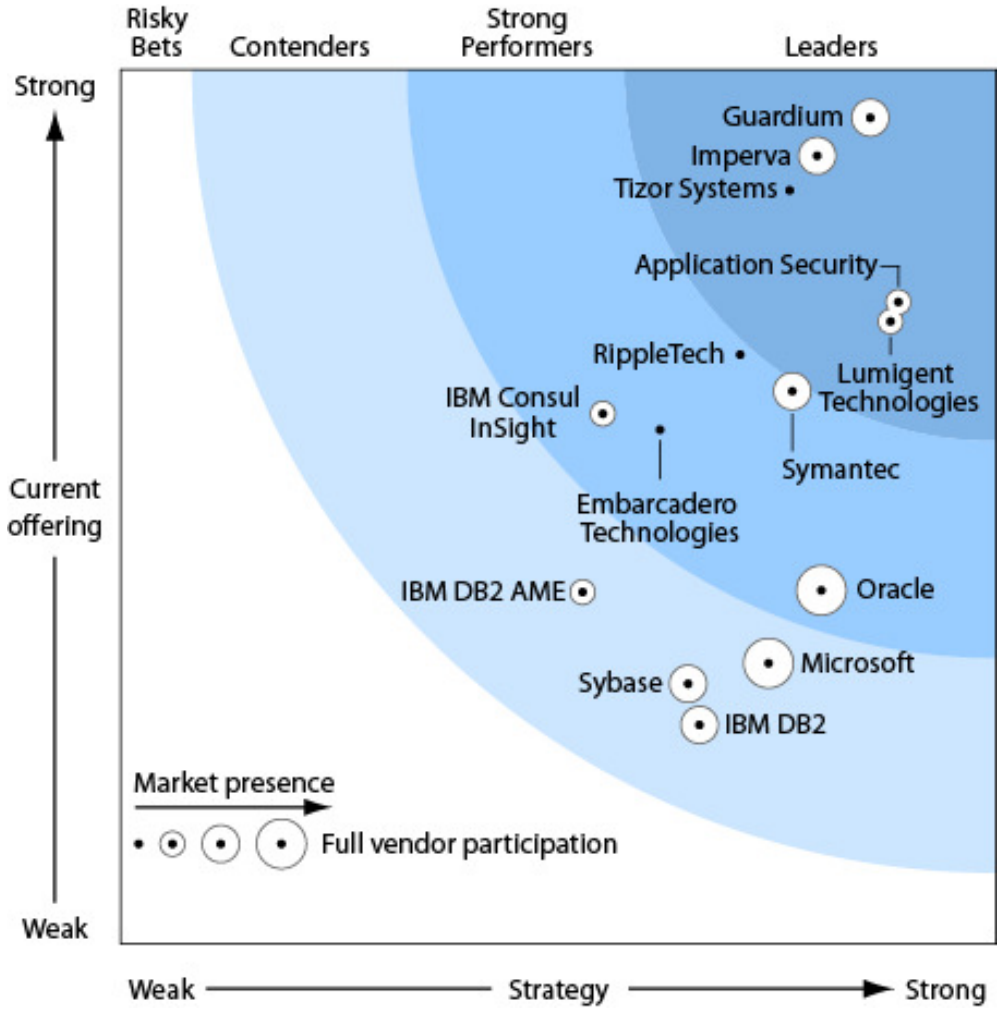
Government

Delaware Criminal Justice Information System
DELJIS
Serving Those Who Serve Others
GOVERNO DA Bahia TERRA DE TODOS NÓS
South African Department of Home Affairs
Ekurhuleni METROPOLITAN MUNICIPALITY
Police Credit
Securing your future
חברת החשמל לישראל
Israel Electric Corp.
המוסד לביטוח לאומי
National Insurance Institute of Israel

Healthcare and Retail

HIGHMARK Blue Cross Blue Shield
Taipei Veterans General Hospital
MEUHEDET Israel's Leading Health Fund
שופרסל

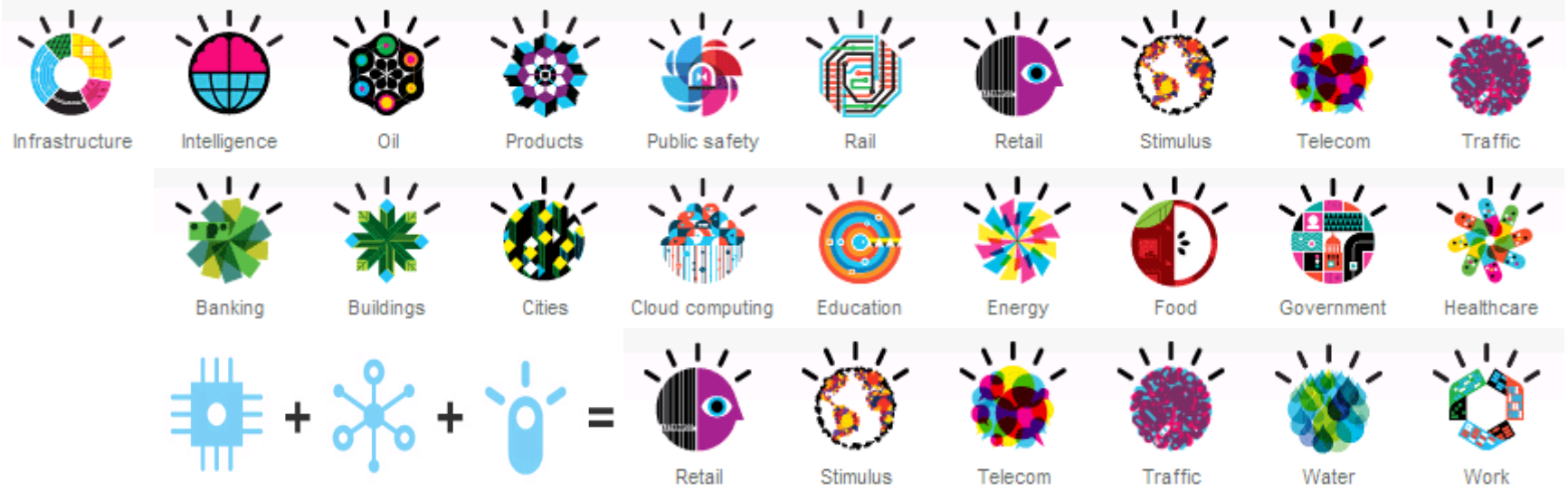
IBM資料庫稽核與防護方案領先其他友商



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

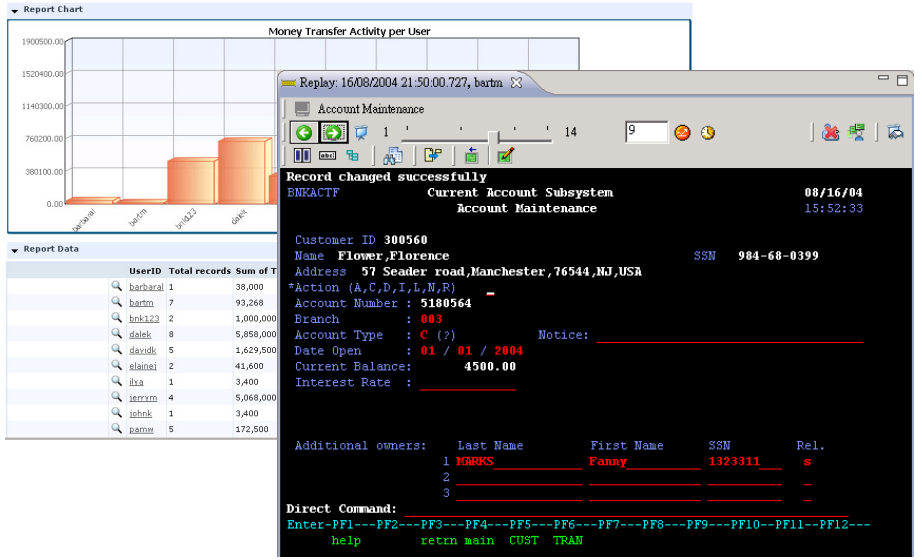
Q & A

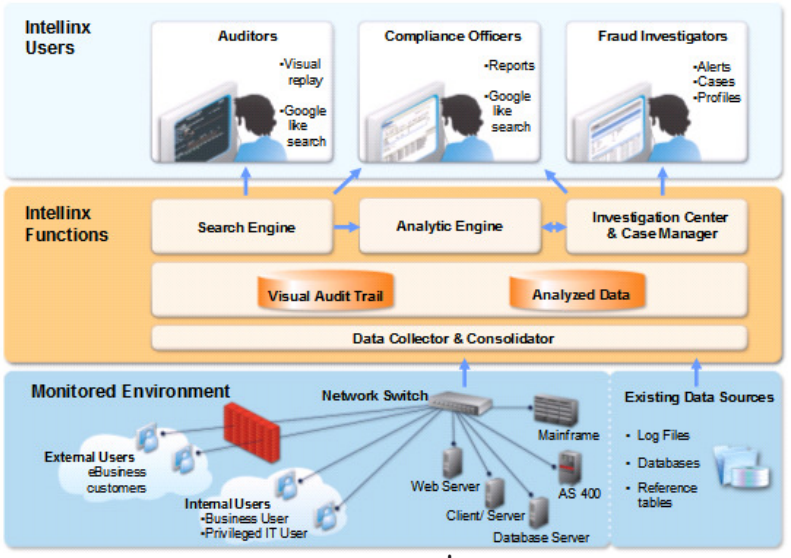
The technology is here.
The people are ready.
The time is now.



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





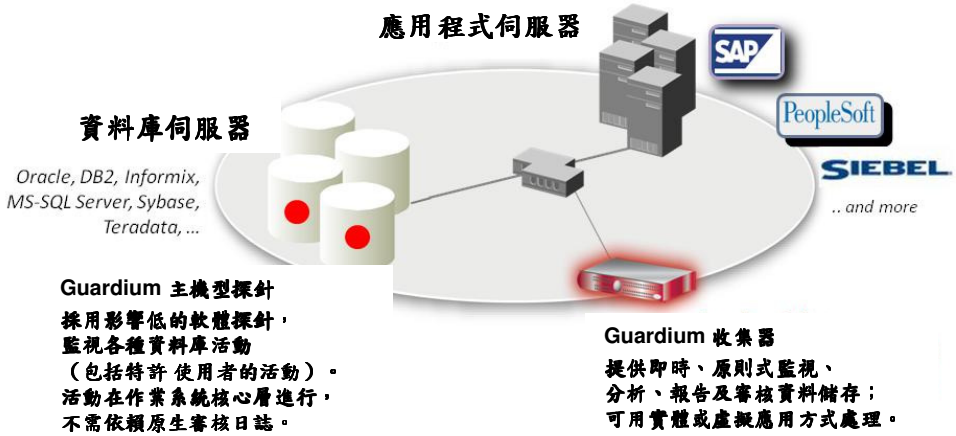
Guardium： 即時資料庫監控、保護、及法規遵循

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。

支援平台

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 (Windows, Unix, z/Linux)	8.1, 8.2, 9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 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