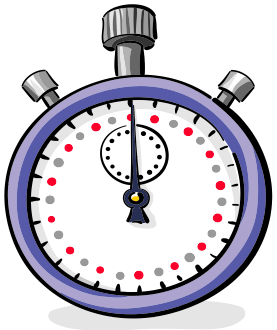
Taifon Your Solution Partner

IBM Guardium 教育訓練
Guardium 產品介紹

泰鋒電腦 洪禮育

簡報綱要

- IBM Guardium產品簡介
- Guardium運作說明
- 問題與討論



IBM Guardium
產品簡介

目前已發生的資安風險

駭客、木馬程式的外部威脅

- ❖購物頻道、網路購物個人資訊外洩
- ❖信用卡網路交易、網路銀行轉帳帳號外洩
- ❖線上遊戲帳號遭竊取.....駭客、詐騙集團盜取.....

最新 | 發燒 | 哇新聞　歷史新聞　書籤　轉寄　列印　討論　推

個資外洩 65%詐騙案在家購物著了道

【聯合報／記者陸倩瑤／專題報導】　2008.06.22 03:04 am

上網拍賣（購物）或電視購物日益普遍，消費者不出門也可以享受瞎拼樂趣，不過一六五反詐欺專線統計資料顯示，便利快速的「無店鋪購物」型態，已成爲消費者個人資料外洩主要管道！

詐騙案件 網購最大宗

消費情報

2008.06.17【工商時報　部]清爭）文／台北報導】

慎防網路個資外洩 遭詐騙

網路購物的危險性在哪？就是個人資料外洩，被詐騙消費者，要消費者再次轉帳，網路購物業者提醒民話，一定要先撥網站上的服務電話確認，千萬別貿然在購物網站上留下資料，後續的物流配送，也有可能

[redacted]受「駭」 5400會員個資外洩

今開放會員查詢帳號是否被竊

〔記者王珮華／台北報導〕國內第[redacted]大購物網站[redacted]昨呼籲使用者盡快更換密碼。該網站表示，上週日晚間遭來自中國的不明人士，以身分證字號輸

內部控管個人資訊外洩的隱憂

- ❖內部客戶資料控管不確實
- ❖委外廠商沒有遵守保密切節協議
- ❖有心人士金錢煽動造成

基測個資外洩 教育部：制度面確實需檢討

中廣新聞網／李人岳 2008-06-18 15:43

前往知識生活大作戰 調整字級：小 中 大 特

國中基測31萬考生的個人資料，傳出被承辦業務的博瑋公司轉漏給補習班，立委質疑考生個資年年外洩，博瑋卻可以連續6年承包基測，其中是不是有官商勾結、內神通外鬼？教育部次長呂木琳表示，制度面確實需要有檢討之處，政風單位也已經介入調查是否有公務員涉案。不過立委還是不滿教育部年年檢討卻還是每年出包！立委要求教育部，把是否通過「資安認證」納爲基測承辦廠商的投標資格。(李人岳報導)

金管會要徹查

【大紀元4月14日訊】

世煌、王昶閔、項程[redacted]無限卡客戶料的對象，金管會官反銀行法四十八條所義務爲由，將對全案[redacted]確有疏失則將[redacted]昨天對此則是低調趙建銘的資料遭到外

[redacted]也強調，若法蒐取這些資料並加以傳播散佈，因此造成[redacted]的損失，[redacted]償。

[redacted]涉嫌高價收購 政商名流個資外洩 第一家庭也受害

中時電子報 www.chinatimes.com 更新日期：2008/04/25 04:33 趙國明台北報導

檢調偵辦政商名流、藝人等個人資料外洩案升高，辦案人員發現《[redacted]》會涉嫌向[redacted]爲首的集團高價收購。調查局台北市調查處廿四日以證人身分，約談該週刊研究組白姓主任等三人到案。

據透露，被外洩個資的政商部分中，令人訝異的是，連第一家庭成員也是受害人。不過，檢調單位對此訊息均保持神祕，不敢冒著洩密罪嫌而出面證實。

由於檢調追查[redacted]販賣個資集團的犯行，是在最近二年，換句話說，《[redacted]》內部人員被約談，也等於是這二年該週刊所刊載出之政商名流、藝人的行蹤及私密的八卦緋聞，都因個資外流而被狗仔捕捉。

資訊安全法規的要求

國際清算銀行(BIS)
新巴塞爾國際協定（New Basel Accord）之作業風險

標準
Accord

Remote
Locations

沙賓法
ISO 27
公司管

Data Center

A1 焦點新聞　台灣優先 自由第一　2008年5月16日／星期五

年度第一 最多人的共同選擇

自由 蘋果

自由時報

創辦人：林榮三　發行人：吳阿明

總社：114台北市瑞光路399號

http://www.libertytimes.com.tw　The LIBERTY TIMES

洩個人資料 朝野共識 最高賠10億

受害民眾索賠 無需舉證

立院司委會 下週一討論

個資外洩嚴重 修法重懲

如何做資料庫稽核

資料庫操作行為的控管

安控人員

操作人員

- ✓ 資安政策改變
- ✓ 可信賴的稽核資訊
- ✓ 即時的警訊控管

稽核人員

- ✓ 權責分明
- ✓ 最佳範例報表
- ✓ 自動化簽送流程

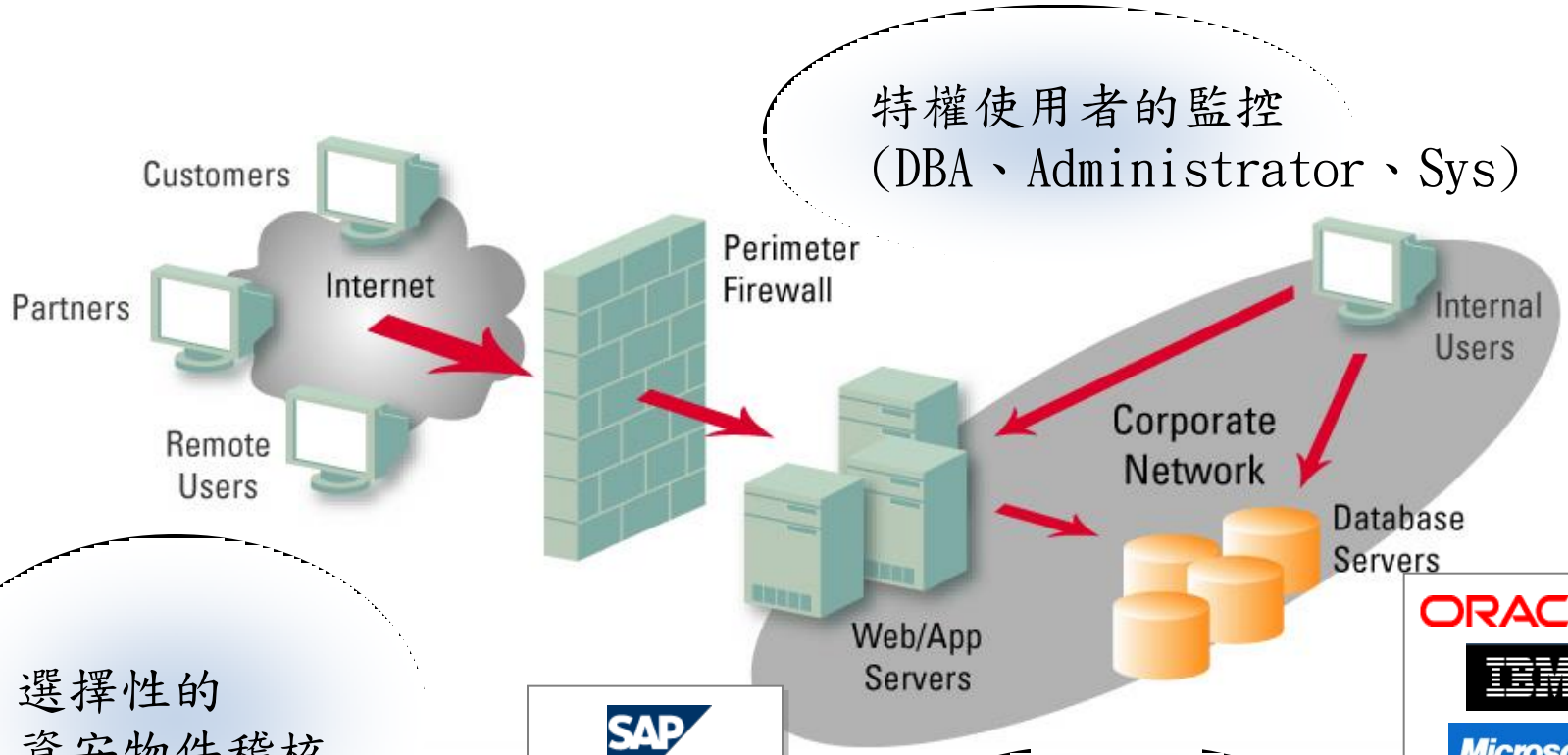
AP/DBA人員

委外廠商

- ✓ 最小的衝擊
- ✓ 變更管理
- ✓ 效能最佳化

Guardium: 100% Visibility & Unified View

資料庫稽核面臨的挑戰


特權使用者的監控
(DBA、Administrator、Sys)
Customers
Partners
Remote Users
Internet
Perimeter Firewall
Internal Users
Corporate Network
Database Servers
Web/App Servers
選擇性的
資安物件稽核
SAP
JDEDWARDS
SIEBEL
PeopleSoft
ORACLE
E-Business Suite
全面性的各種不同
資料庫的稽核
ORACLE
IBM
Microsoft
SYBASE
Informix

追溯資料庫的行為事件

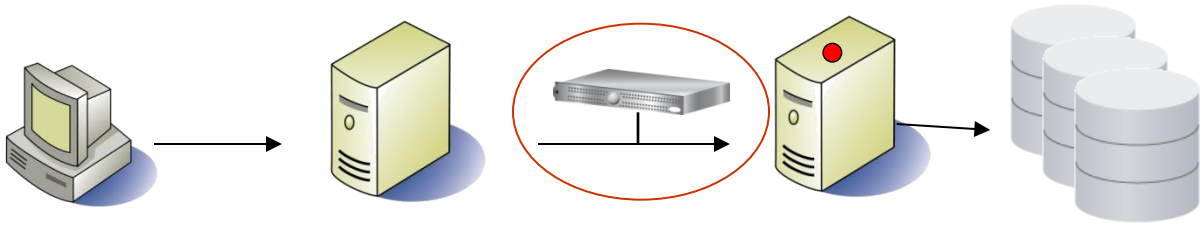
❖在追溯資料庫資訊安全的前提之下，還原整個資料庫的行為事件必須要還原的五大要素：

- WHO
- WHAT
- WHERE
- WHEN
- HOW

誰在什麼地方使用了什麼工具在什麼時候做了什麼事情?

追溯資安事件的五大要素

所有的 SQL 指令可以根據其上下文的關聯性，即時的被分析過濾分類，並提供特定的資訊給稽核人員



Client IP
OS user ID
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
App user ID
Access programs

ALL SQL commands
Fields
Objects
Verbs
DDL
DML
DCL
DB user ID
DB version
DB type
DB protocol
Ports
SQL errors
SELECTs
Bind values

稽核人員要看的資料-1

- 一般而言 IDS/IPS/Firewall 也可以根據這些“威脅特徵”來偵測紀錄這些資料庫的行為
- 這些偵測威脅特徵得到的紀錄可讀性不佳
- IDS/IPS/Firewall 看到的資料是：

```
00000000 : 00 53 d0 51 00 01 00 4d 20 0d 00 44 21 13 53 41    .S.Q...M ..D!.SA
00000010 : 4d 50 4c 45 20 20 20 20 20 20 20 20 20 20 20 20    MPLE
00000020 : 4e 55 4c 4c 49 44 20 20 20 20 20 20 20 20 20 20    NULLID
00000030 : 20 20 54 4f 4f 4c 33 45 30 30 20 20 20 20 20 20    TOOL3E00
00000040 : 20 20 20 20 41 41 41 41 41 61 48 53 00 01 00 05    AAAAAaHS....
00000050 : 21 16 f1 00 29 d0 03 00 01 00 23 24 14 00 00 00    !...).....#$....
00000060 : 00 19 73 65 6c 65 63 74 20 2a 20 66 72 6f 6d 20    ..select * from
00000070 : 52 75 6c 65 31 44 72 6f 70 20 20 ff                Employee
```

稽核人員要看的資料-2

- 這個指令是給資料庫管理人員看的：

UPDATE TEST_SQL SET TEXT='SELECT * FROM USER_OBJECTS UNION SELECT * FROM USER_OBJECTS WHERE ID=11;

- 可讀性是比使用IDS/IPS 好一些
- 將五大要素分類歸類不是更好

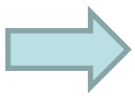
This....

Dsfrgdfgw4tsfdfsgsdfgfdgsdfg

Ooxxjr0172-gfhfhsfhsdfhhgsfgh50=jdsfh'adsf-815

Asdl54k;sadfu8-asdf

Lkasdjflasdf80732-58-adsfpkasdf



into

Who : guest

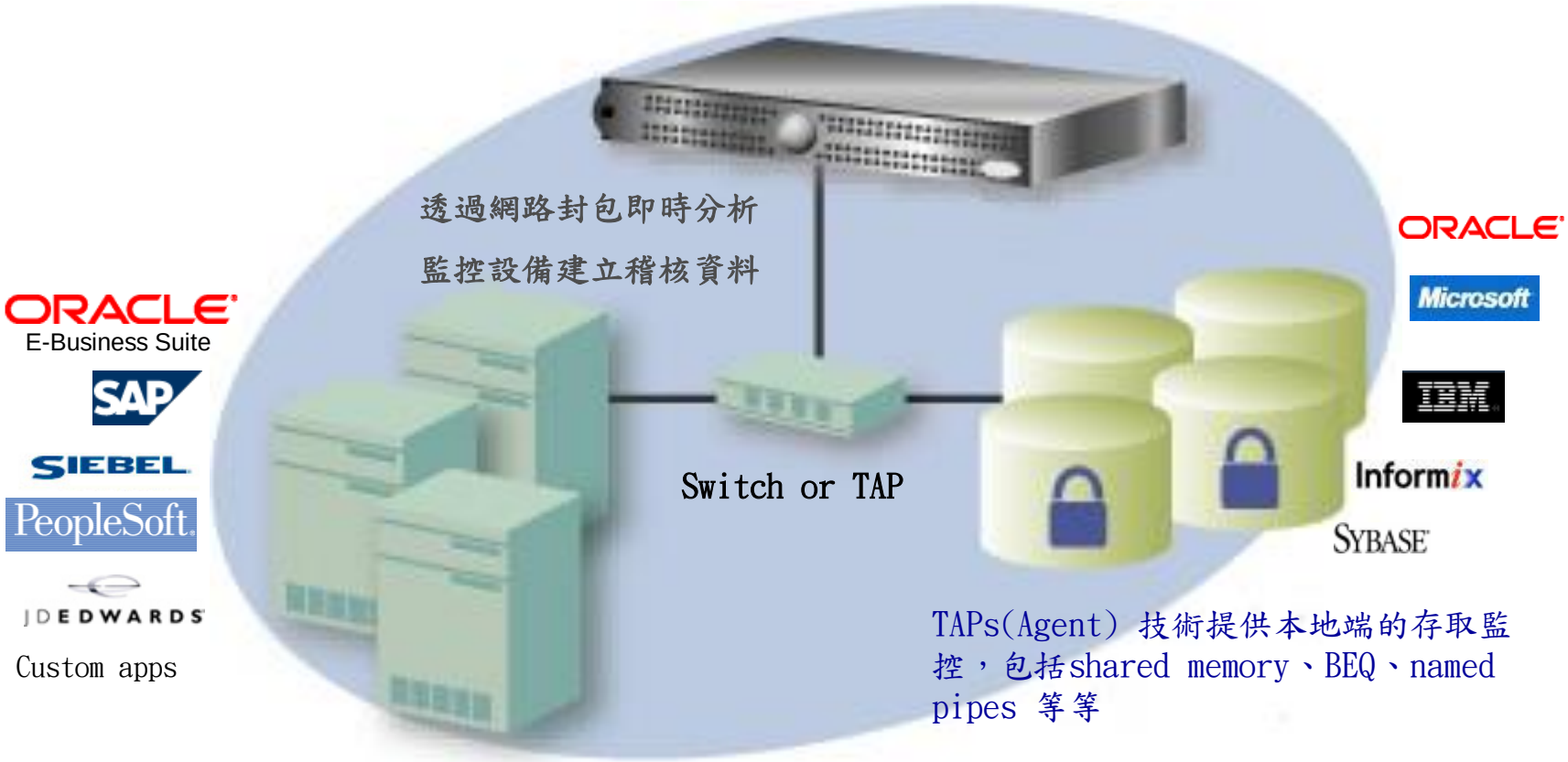
What : SAP ERP SYSTEM

Where :200.151.21.103

When : 2007/01/02 22:14:23

How : update "account" set "amount" = '10000000' where name like 'John Doe'

解決方案：Guardium SQL Guard



- 非侵入性
- 權責分明
- 跨平台
- 自動化&集中管理

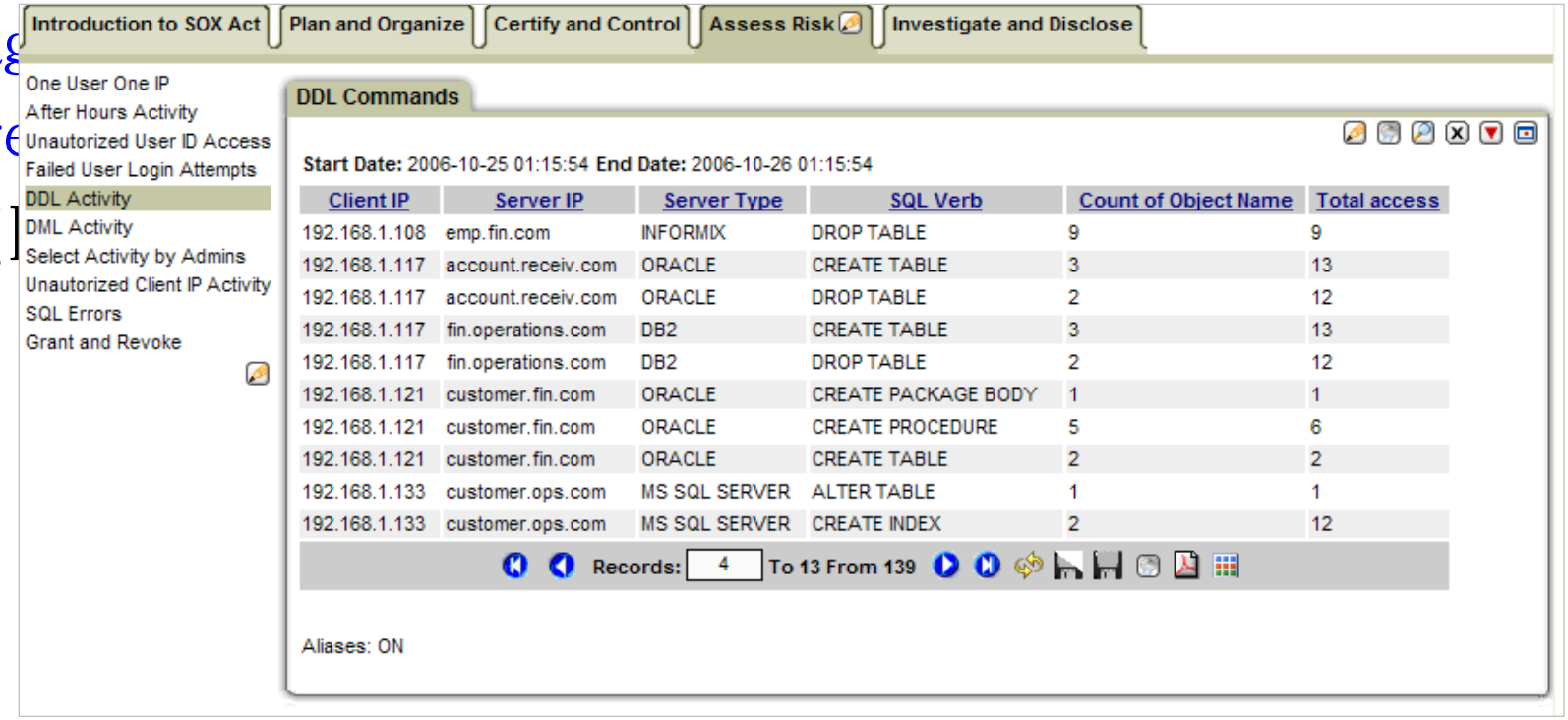
Guardium SAFEGUARDING DATABASES™ 公司簡介

- 成立於2002年

- 主要由Cisco以及其他大型國際性投顧公司投資
- 唯一可即時保護資料庫，並自動化所有資安法規(SOX、PCI、Basel II、Data Privacy)流程的完整解決方案
- 唯一全心全力只做”資料庫稽核”的公司
- IBM公司收購成為旗下之一資安軟體

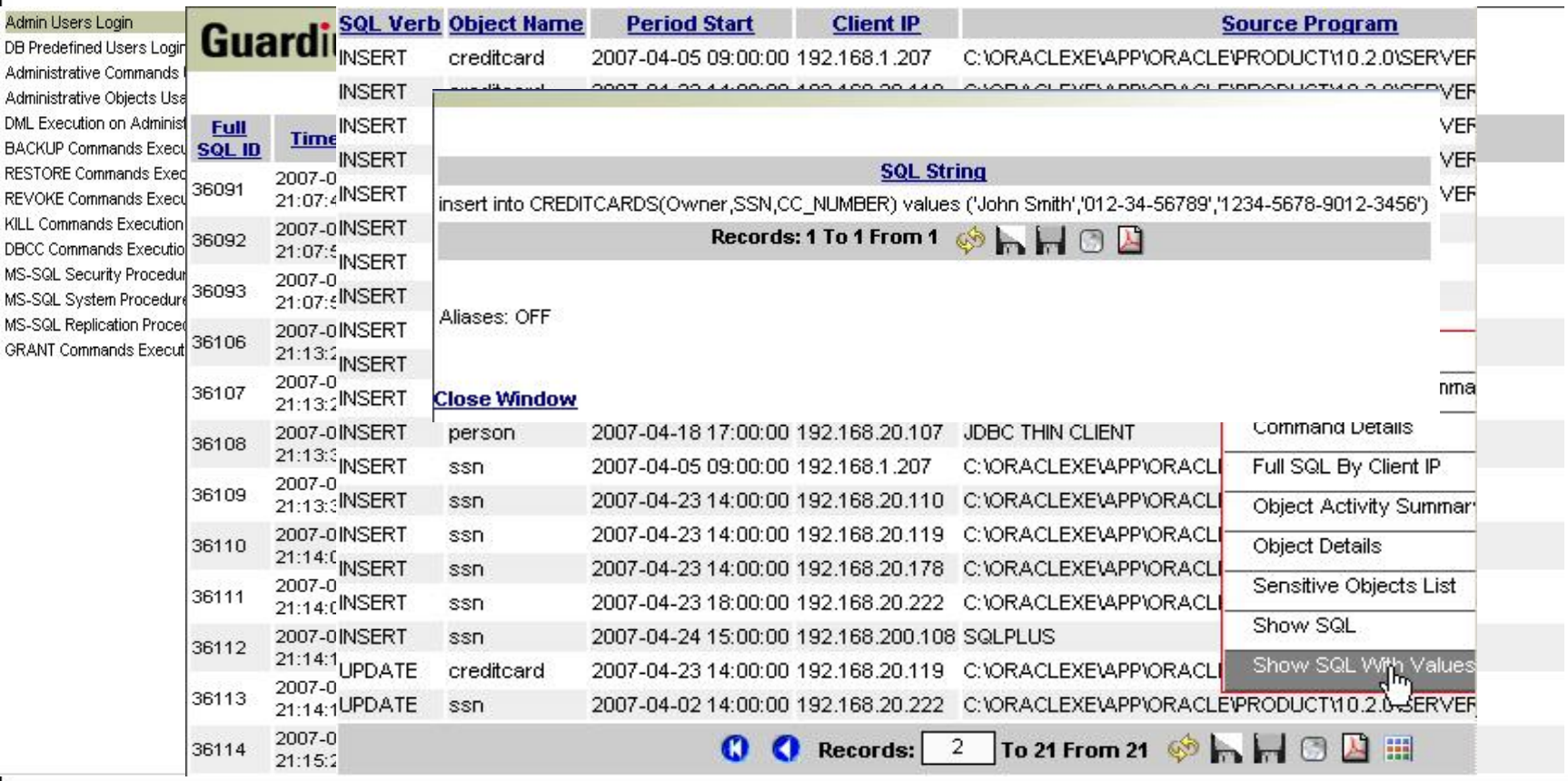
符合國際法規最佳範例的報表

- 四大會計事務所(KPMG、PWC、DTT、EY) 認可 100% 符合 Data privacy、SOX & PCI 法規的報表
  - Based on industry best practices
  - Drag
  - Thre
- 毋須



徹底稽核資料庫的活動行為

- 保護敏感性資料的流出和遭受到竄改，記錄下所有對資料庫的存取行為：**誰**在**什麼地方**使用了**什麼工具**在**什麼時候**做了**什麼事情**?

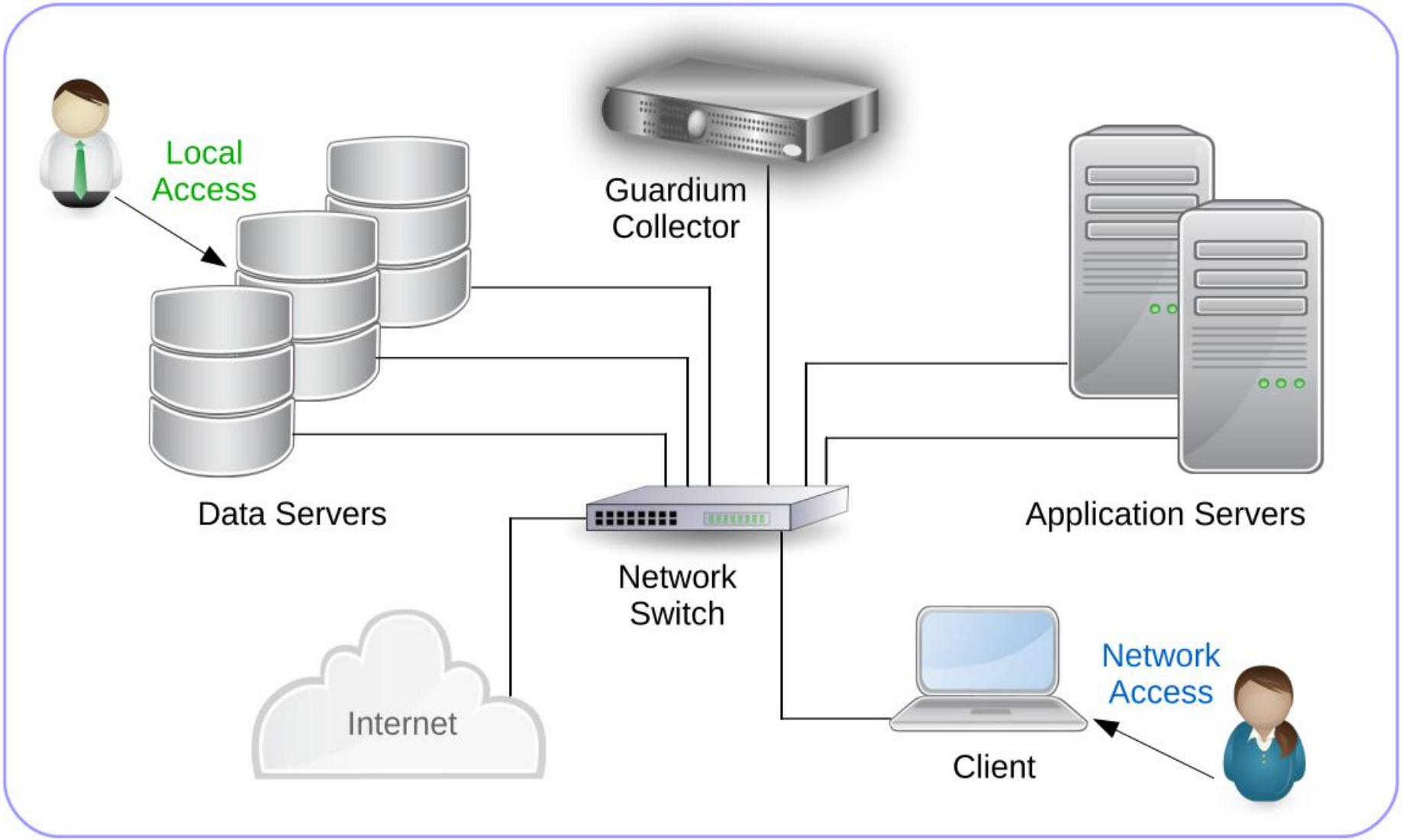


支援的資料庫版本

Supported DBMS	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 LUW (Windows, Unix, z/Linux)	8.0, 8.2, 9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9, 9.5, 9.7
IBM DB2 LUW for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10,11, 11.5
MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreeSQL	8
Teradata	6.x, 12, 13

Guardium 運作說明

標準Guardium 環境建置

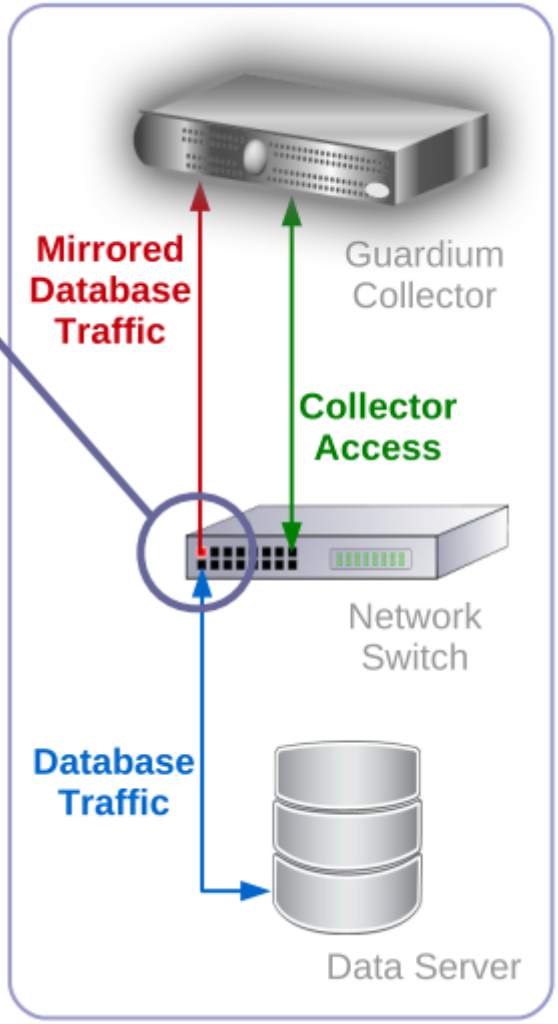


Guardium 監控方式一: Port Mirror

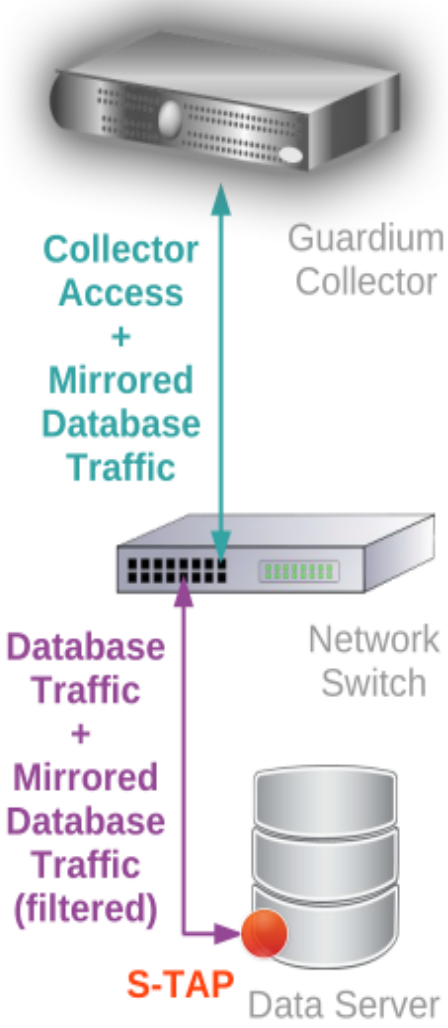
Copy of network packets observed on the switch port connected to the data server is sent to the Collector

- No impact on data server performance
- Requires network switch with port mirroring:
  - Switched Port Analyzer (SPAN)
  - Roving Analysis Port (RAP)
- Requires direct connection to the Collector
- Existing switch may not be able to accommodate multiple data servers connected to that switch
- Added cost of network switch with port mirroring feature
- Encrypted and local connections will not be monitored

Only recommended if network hardware already exists and data server cannot handle any additional software load



Guardium 監控方式二:Software Tap (S-TAP)



Host-based DBMS-independent software agent that sends network and local database activities to Collector

- Monitors all database activities at Operating System level:
  - TCP, Shared Memory, Named Pipes, Bequeath
- Handles encrypted traffic:
  - SSH/IPSEC, Oracle ASO, SQL Server SSL
- Does not require any changes to database environment
- Installed only once on every system regardless of how many database instances and types are running on that system
- No additional hardware cost and lower implementation cost
- Specific traffic can be filtered such that not all traffic is sent to the Collector. This reduces network load significantly.
- Less than 5% performance impact on data server

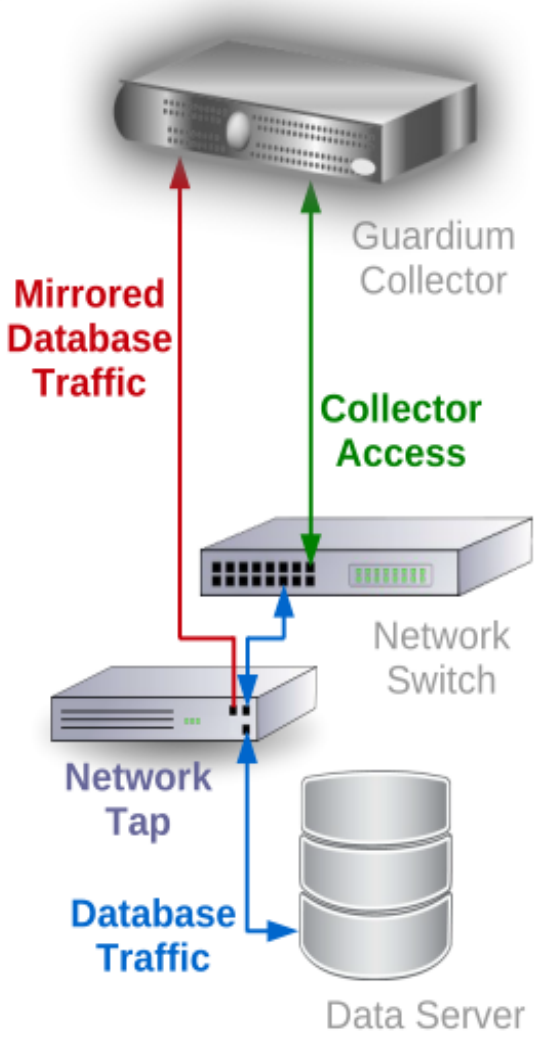
S-TAP is the recommended database activity monitoring option

Guardium 監控方式三: Network Tap

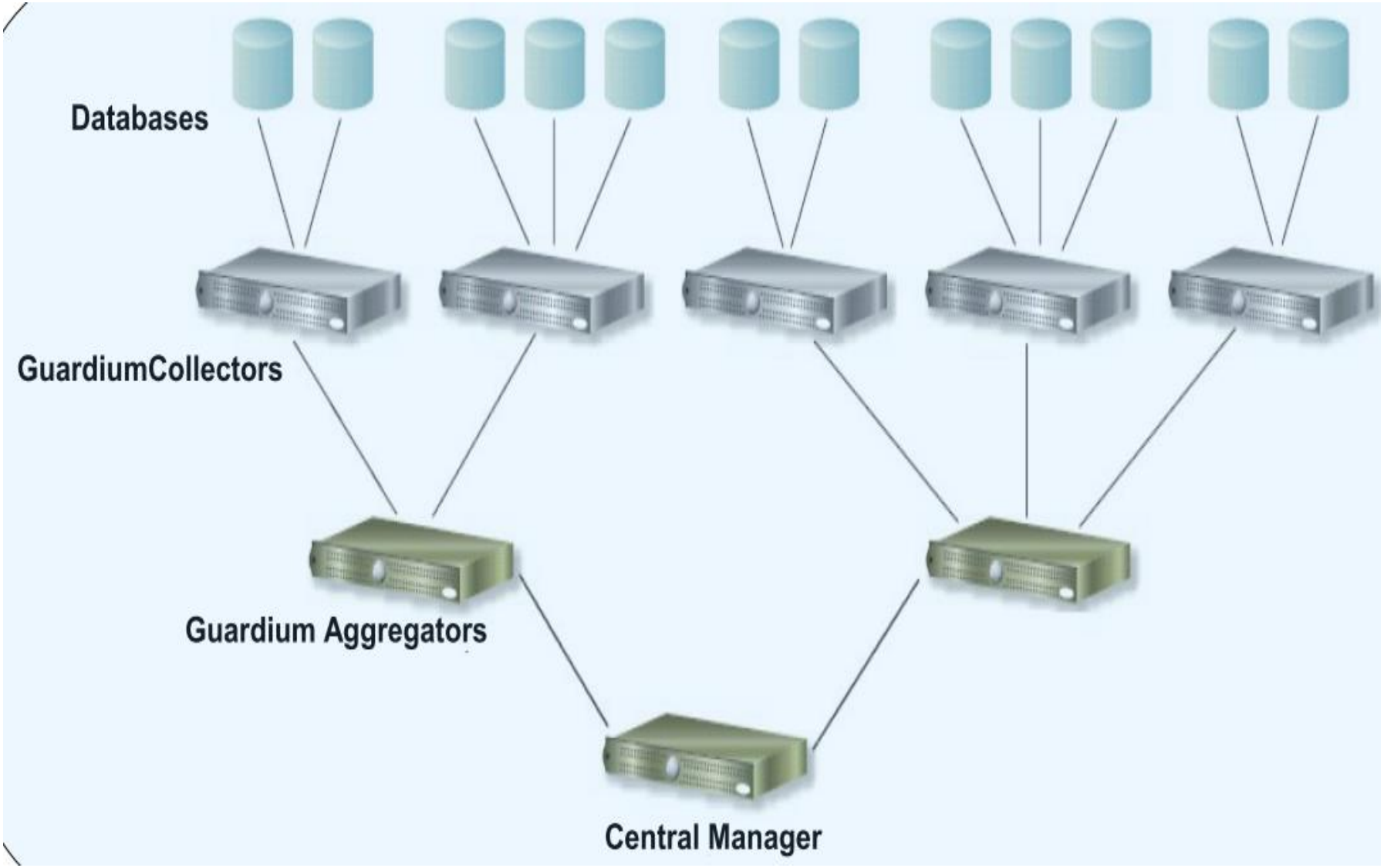
Dedicated network tap hardware sends copy of data server traffic is to Collector (similar to port mirroring)

- No dependency on existing network hardware
- No impact on data server performance
- Added cost of network tap for each data server
- Requires direct connection to the Collector
- Data server has to be taken offline for installation
- Encrypted and local connections will not be monitored

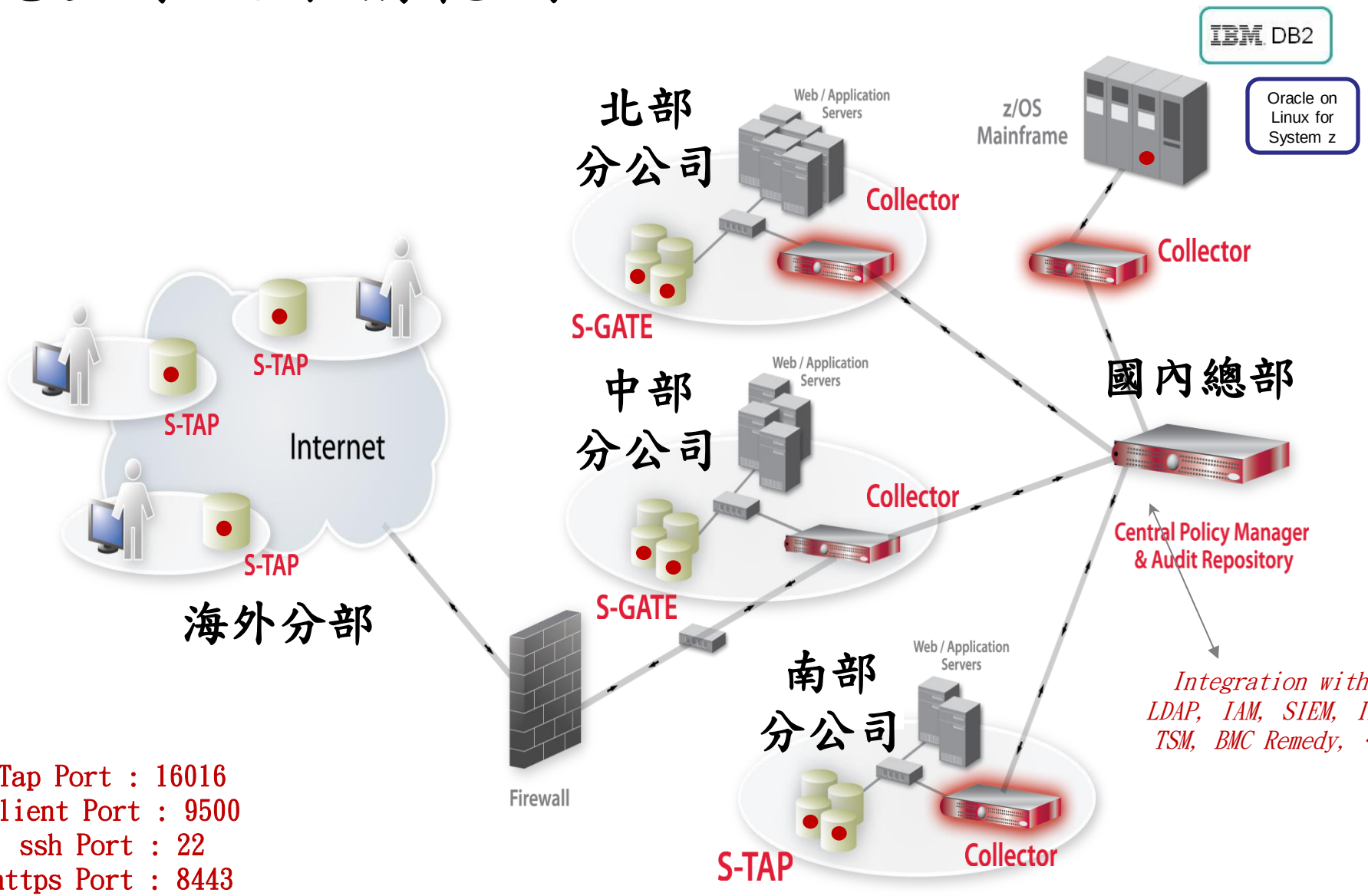
Only recommended if data server has a high load and cannot handle any additional software load



資料集中化管理


Databases
GuardiumCollectors
Guardium Aggregators
Central Manager

完整系統架構範例



Tap Port : 16016
Client Port : 9500
ssh Port : 22
https Port : 8443
Others : FTP、SCP

稽核資料中長期保存

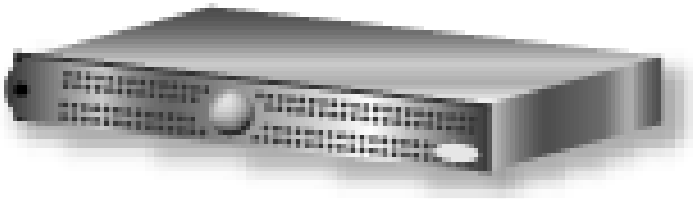

```
g7s.guardium.com> store storage-system Centera backup on
ok
g7s.guardium.com> store storage-system Centera archive on
ok
g7s.guardium.com> store storage-system TSM archive on
ok
g7s.guardium.com> store storage-system TSM backup on
ok
g7s.guardium.com>
```

Guardium 自我監控機制

系統
- 正常運行時間&再啟動
- 磁碟空間 (%滿)
- CPU 負載
- 記憶體使用量
- 失敗的登錄

內部的資料庫
- 狀態: 升高/ 下降
- 磁碟空間 (%滿)
- 系統資源
- 現行運作的疑問
- 回應時間

檢視 Engine (snif)
- 狀態: 升高/下降/超出負荷
- CPU & memory 使用狀況
- 認定的基準
- 失去的請求
- 規則和結構配置變更



Guardium 使用者行動
- 登入 / 登出
- Full Audit Trail
- 資料層級的安全
- 應用軟體層級的安全
- 憑證變更

收集程序
- S-TAP
- CAS
- Data Upload (Domains)
- LDAP Imports

網路伺服器 & 應用軟體
- 狀態: 升高/ 下降
- Scheduled Jobs Exceptions
- Audit processes
- Correlation alerts
- Configuration changes
- CAS templates
- Auto Detect process
- Classification process
- Vulnerability Assessment

Database Activity Patterns
- Database types
- Database Servers
- Session/SQL Count
- Activity rates
- Ignored data

Q & A 問題與討論