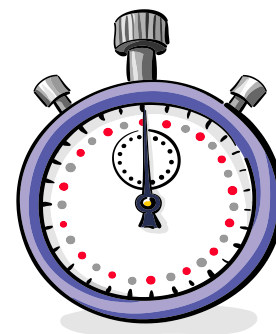


IBM Guardium 教育訓練  
Guardium 產品介紹

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，已成為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

## 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】國內第一大購物網站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

前往知經生活大作戰 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樟公司洩漏給補習班，立委質疑考生個資年年外洩，博樟卻可以連續8年承包基測，其中是不是有官商勾結、內神通外鬼？教育部次長呂木添表示，制度面確實需要檢討之處，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外包！立委要求教育部，把是否通過「資安認證」納為基測承辦廠商的投標資格。(李人岳報導)

法蒐取這些資料並加以傳播散佈，因此造成[ ]的損失，[ ]償。

## 金管會要徹查

【大紀元4月14日訊】

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

[ ]也強調，若

## [ ]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 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《[ ]》曾涉嫌向[ ]為首的集團高價收購。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[ ]下販賣個資集團的犯行，是在最近二年，換句話說，《[ ]》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。

[ ]的目擊者



# 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

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

719,335

511,0019

自由 蘋果

創辦人：林榮三

發行人：吳阿明

# 自由時報

發行所：台北市中山路744號

總社：114台北市瑞光路399號

今日氣象

北部地區	22°C-28°C
中部地區	22°C-30°C
南部地區	22°C-30°C
高屏地區	24°C-31°C

台北市 22°C-27°C

桃園山 17°C-21°C

新竹地區 22°C-28°C

苗栗地區 24°C-31°C

基隆 22°C-28°C

花蓮地區 24°C-31°C

台東地區 24°C-31°C

澎湖地區 24°C-31°C

金門地區 24°C-31°C

馬祖地區 24°C-31°C

民國紀事

農曆4月12日(丙辰)

宜：祭祀、祈禱、嫁娶、安葬

忌：造灶、安葬

## 洩個人資料

## 朝野共識 最高賠10億

**受害民衆索賠 無需舉證**

草案第二十九條也規定，受害民衆索賠時，不須負舉證責任，但非公務機關要證明「無故意或過失責任」才能免責，公務機關則須負「無過失責任」；草案第三十二條同時賦予縣市政府有「行政檢查權」，不須透過法院審查程序，即可查扣企業非法所有的個人資料。

由於駭客入侵公私機關電腦，竊取個人資料層出不窮，法務部官員指出，依草案規定，公務機關只有在天災、地震等不可抗力才能免責，否則須負「無過失責任」，但非公務機關只要能證明窮盡一切方法，仍無法防止駭客竊取資料，就能免責。

至於草案規範對象，法務部官員形容為「包山包海」，不限行規定的公務機關和電信、醫院、電信等業，只要使用電腦或書面處理個人資料，統統在保護範圍。(相關新聞詳刊B6)

**立法院委會 下週一討論**

現行「電腦處理個人資料保護法」規定，如民眾個人資料外洩，最高總額可索賠二千萬元，行政院版草案提高到五千萬，國民黨立委謝國樑等人版本則無賠償上限；至於外洩每人每一事件僅金，現行法律和草案規定以十萬元到二萬元內計算，法務部傾向降低到五百元。

司法院指出，現今個資外洩情形嚴重，限額五千萬元太低，大企業可能認為無關痛癢，但無限賠償又可能導致企業倒閉，衍生出社會問題，因此建議草案第二十八條規定上限為十億元，法務部評估後認為民眾應可接受。

部也表支持，上述機關一致認為，公務和非公務機關使用民眾個人資料情形普遍，應加重賠償責任，才能保護民眾隱私權；由於全案已有共識，下週一立法院委員會將開始逐條討論。

**個資外洩嚴重 修法重懲**

立法院相關官員說，法案依此通過後，未來若再發生重大個資外洩案，被告勢必面臨過億或動輒高達數億元的超高賠償。

官員舉例，近年發生的電視購物頻道、網路書店，或衛生署疾病管制局不慎洩漏民眾病歷等重大外洩個案，如果未來修法後出現類似前述如此大規模的個資外洩案，個案被告很可能就會遭到億元以上的鉅額賠償。

全案目前不僅獲朝野立委同意，法務

沙賓法 ISO 27 公司管

Data Center

# 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

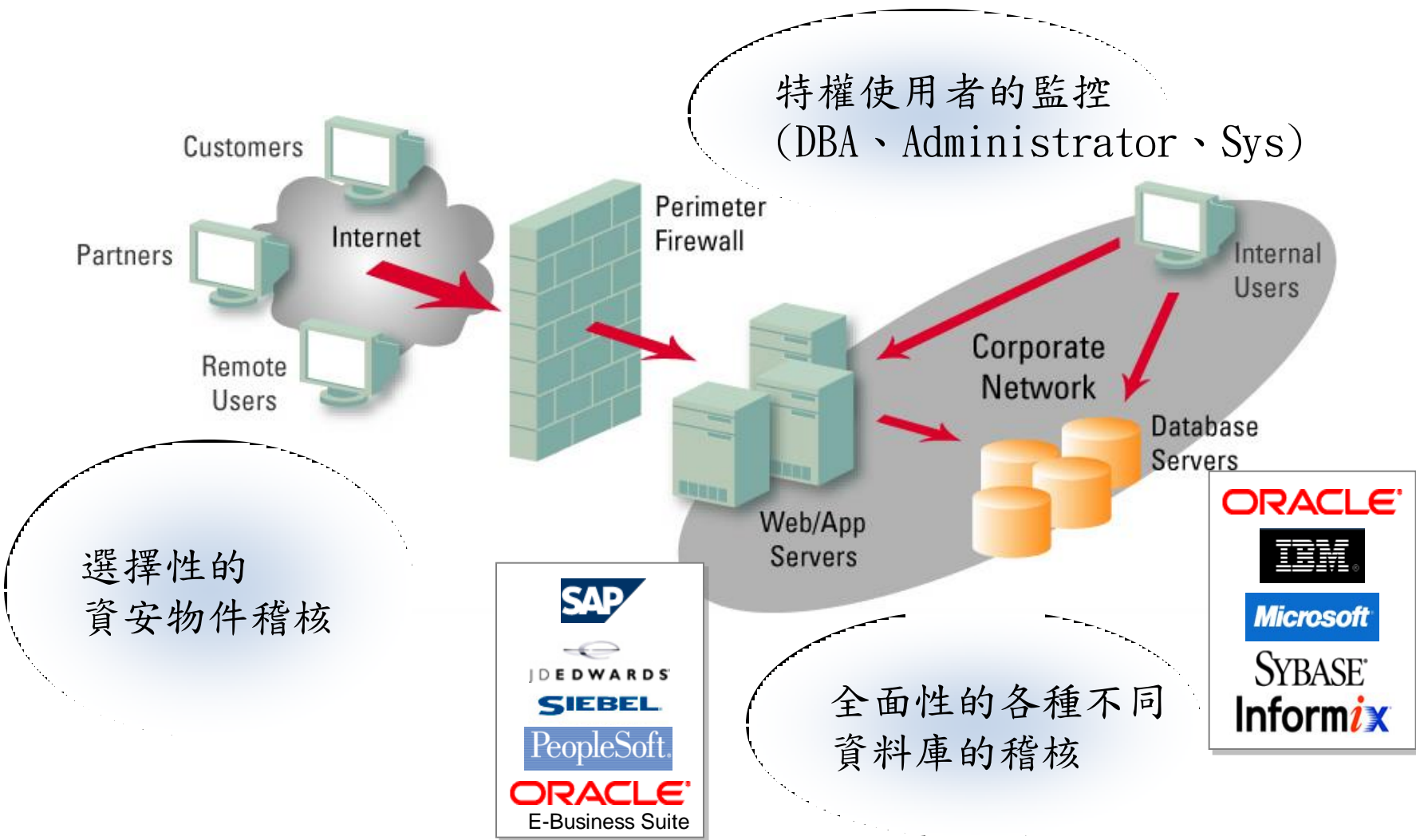


AP/DBA人員  
委外廠商

- ✓ 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



# 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

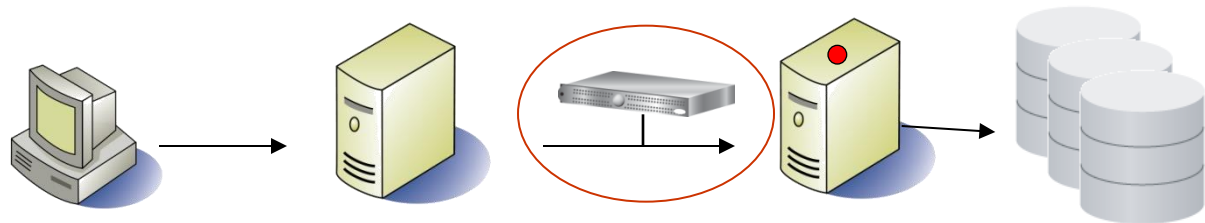
■ WHEN

■ 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	MPLE
00000020 : 4e 55 4c 4c 49 44 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	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 is 比使用 IDS/IPS 好一些

❖ 將五大要素分類歸類不是更好

This....

Dsfrgdfgw4tsdfsgsd  
fgfdgsdfg

Ooxxjr0172-  
gfhfhsfhsdfhhgs  
fgh50=jdsfh'adsf  
-815

Asdl54k;sadfu8-asdf

Lkasdjflasdf80732-  
58-adsfpkasdf



into

Who : guest

What : SAP ERP SYSTEM

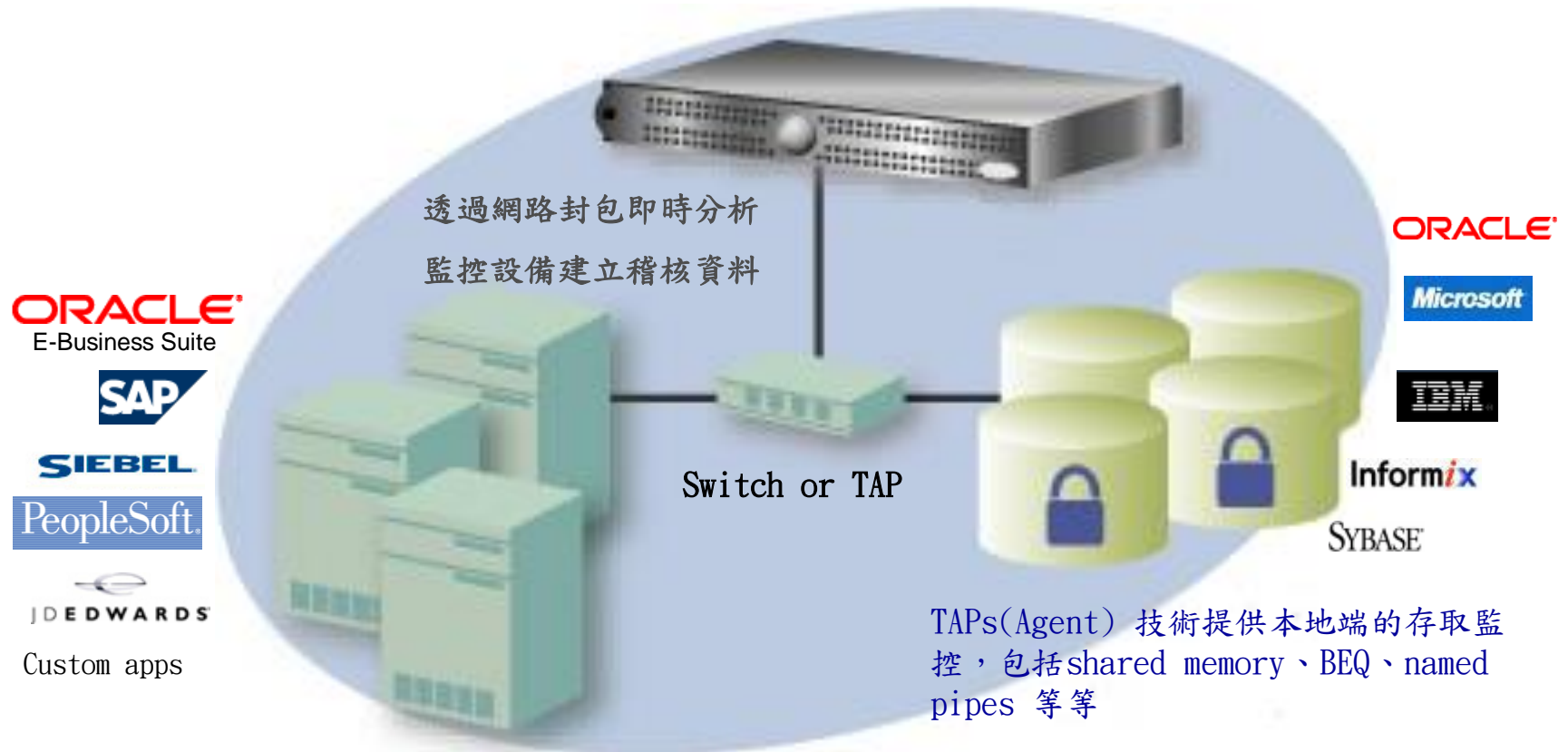
Where :200.151.21.103

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

How : update "account" set "amount" =  
'1000000' 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® 公司簡介

SAFEGUARDING DATABASES™

❖ 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

Introduction to SOX Act | Plan and Organize | Certify and Control | Assess Risk | Investigate and Disclose

DDL Commands

Start Date: 2006-10-25 01:15:54 End Date: 2006-10-26 01:15:54

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
192.168.1.108	emp.fin.com	INFORMIX	DROP TABLE	9	9
192.168.1.117	account.receivev.com	ORACLE	CREATE TABLE	3	13
192.168.1.117	account.receivev.com	ORACLE	DROP TABLE	2	12
192.168.1.117	fin.operations.com	DB2	CREATE TABLE	3	13
192.168.1.117	fin.operations.com	DB2	DROP TABLE	2	12
192.168.1.121	customer.fin.com	ORACLE	CREATE PACKAGE BODY	1	1
192.168.1.121	customer.fin.com	ORACLE	CREATE PROCEDURE	5	6
192.168.1.121	customer.fin.com	ORACLE	CREATE TABLE	2	2
192.168.1.133	customer.ops.com	MS SQL SERVER	ALTER TABLE	1	1
192.168.1.133	customer.ops.com	MS SQL SERVER	CREATE INDEX	2	12

Records: 4 To 13 From 139

Aliases: ON



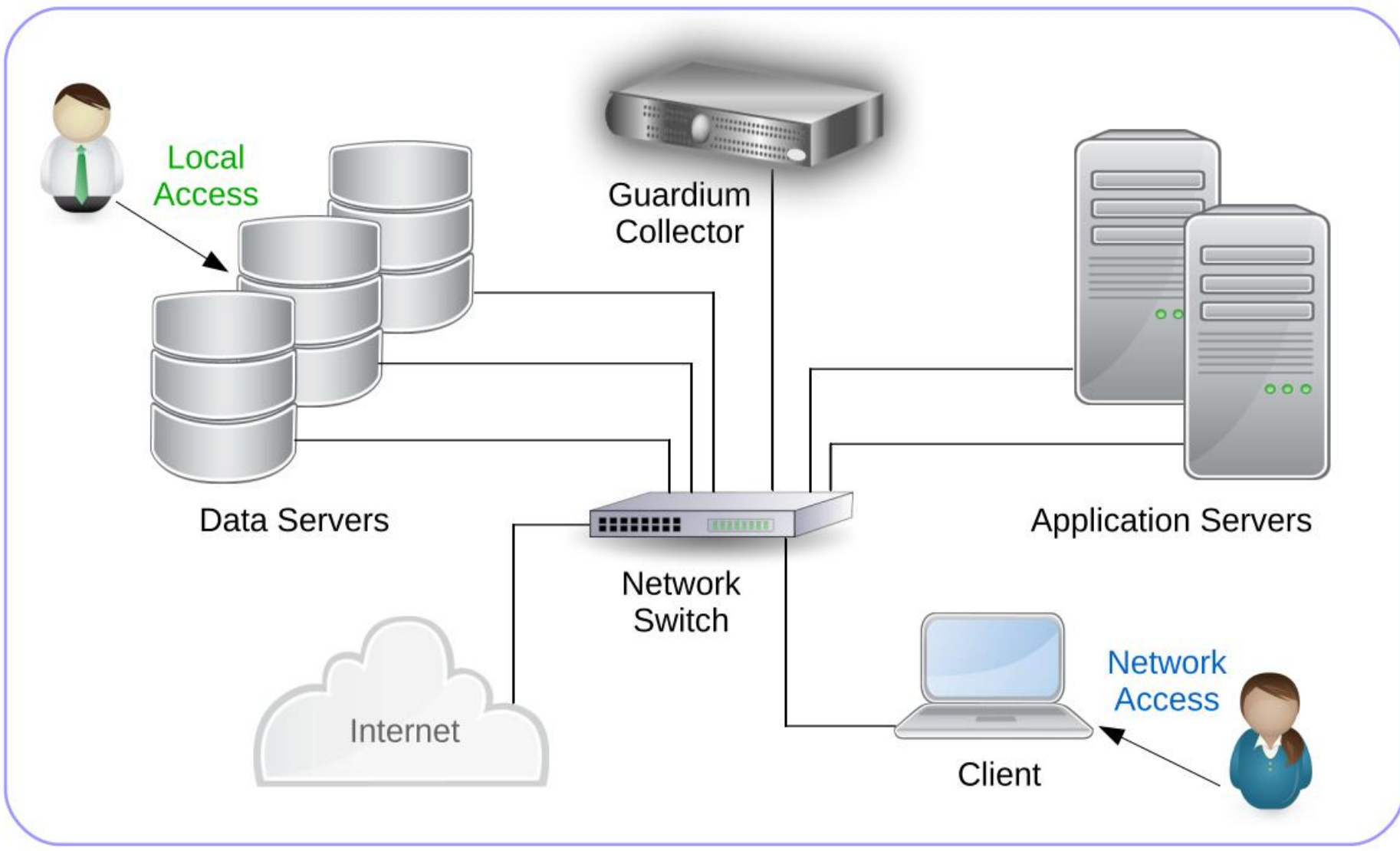
# 支援的資料庫版本

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
PostgreSQL	8
Teradata	6.x, 12, 13

# Guardium 運作說明



# 標準Guardium 環境建置

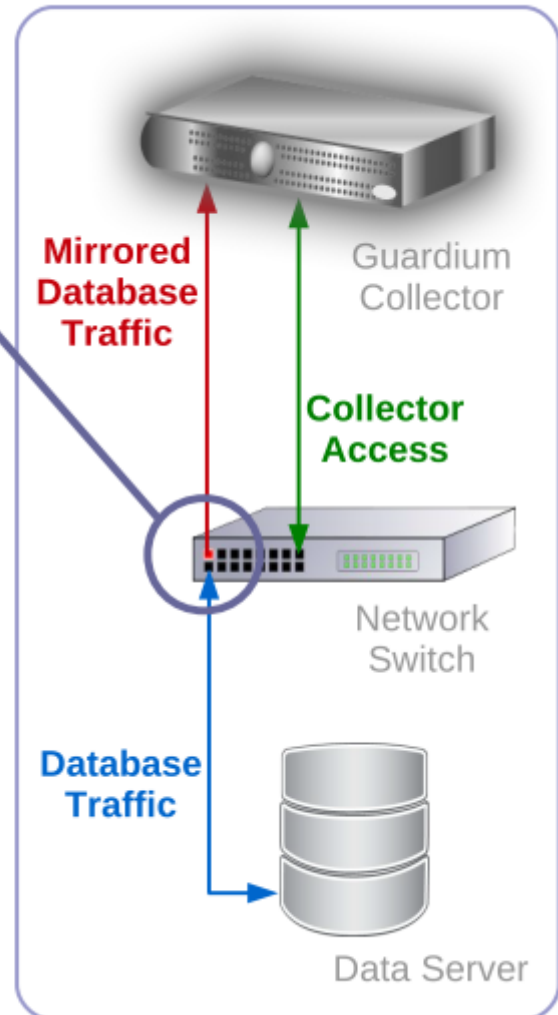


# Guardium 監控方式一：Port Mirror

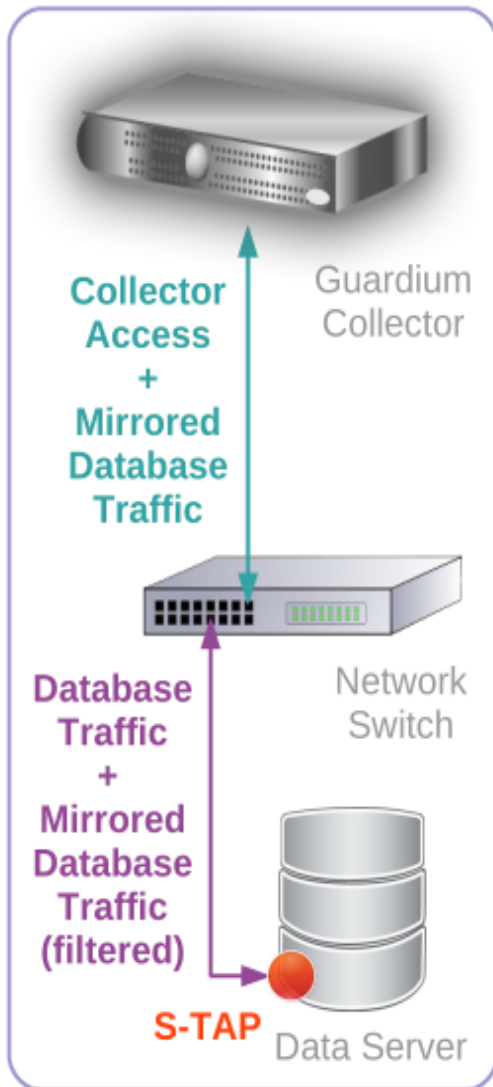
**Copy of network packets observed on the switch port connected to the data server is sent to the Collector**

- 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

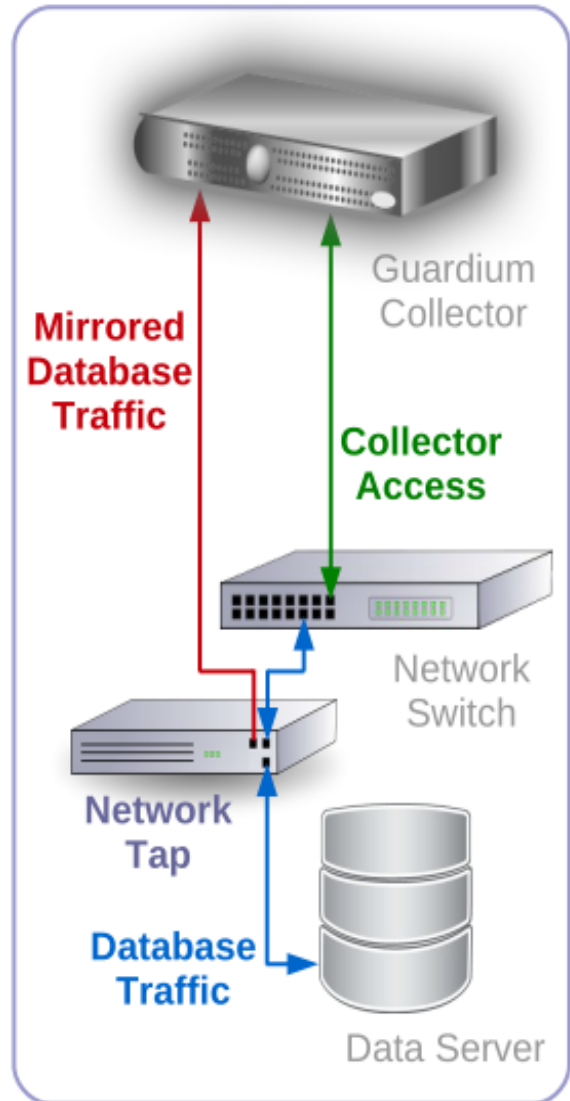
S-TAP is the recommended database activity monitoring option

## Guardium 監控方式三：Network Tap

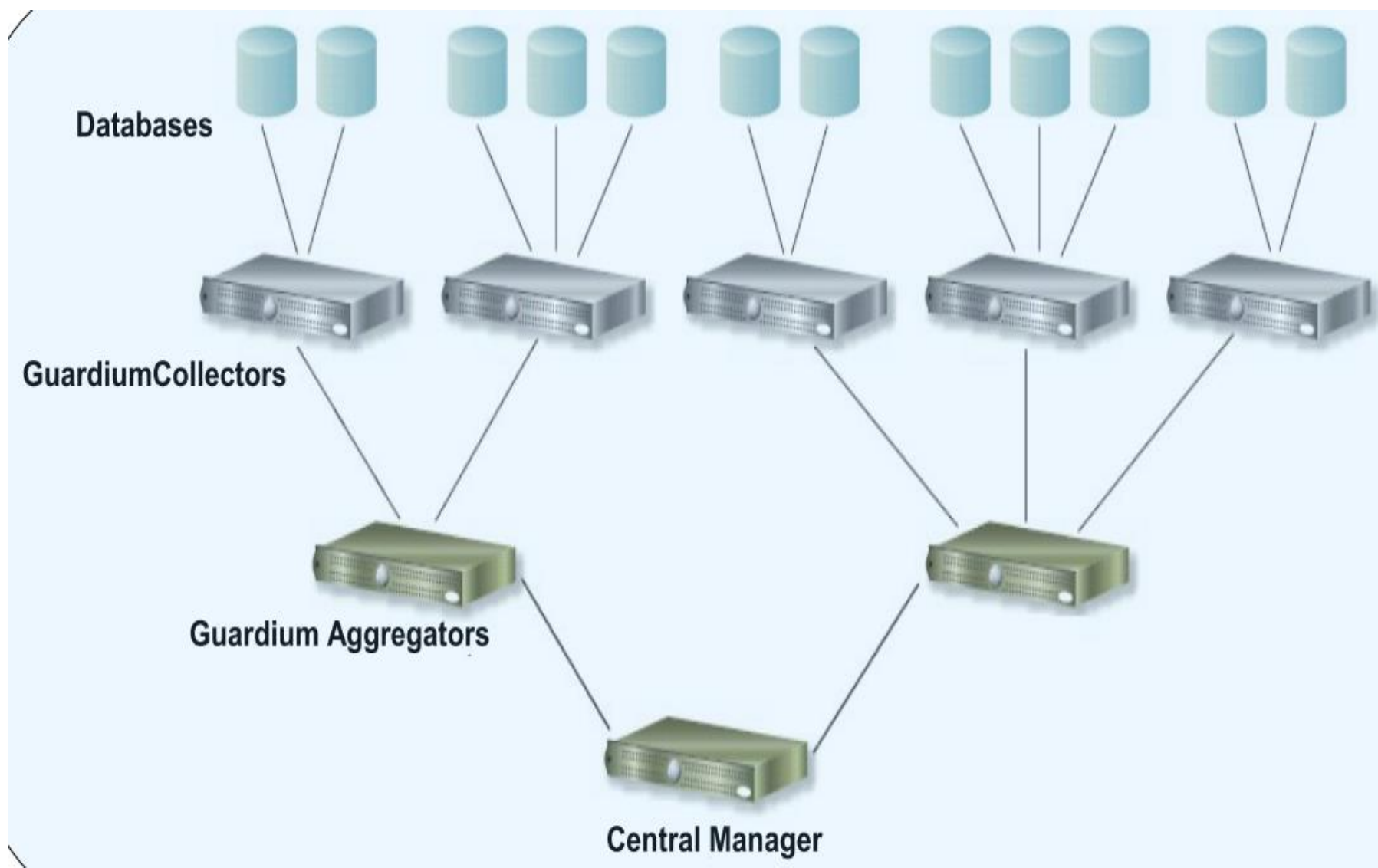
**Dedicated network tap hardware sends copy of data server traffic is to Collector (similar to port mirroring)**

- 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

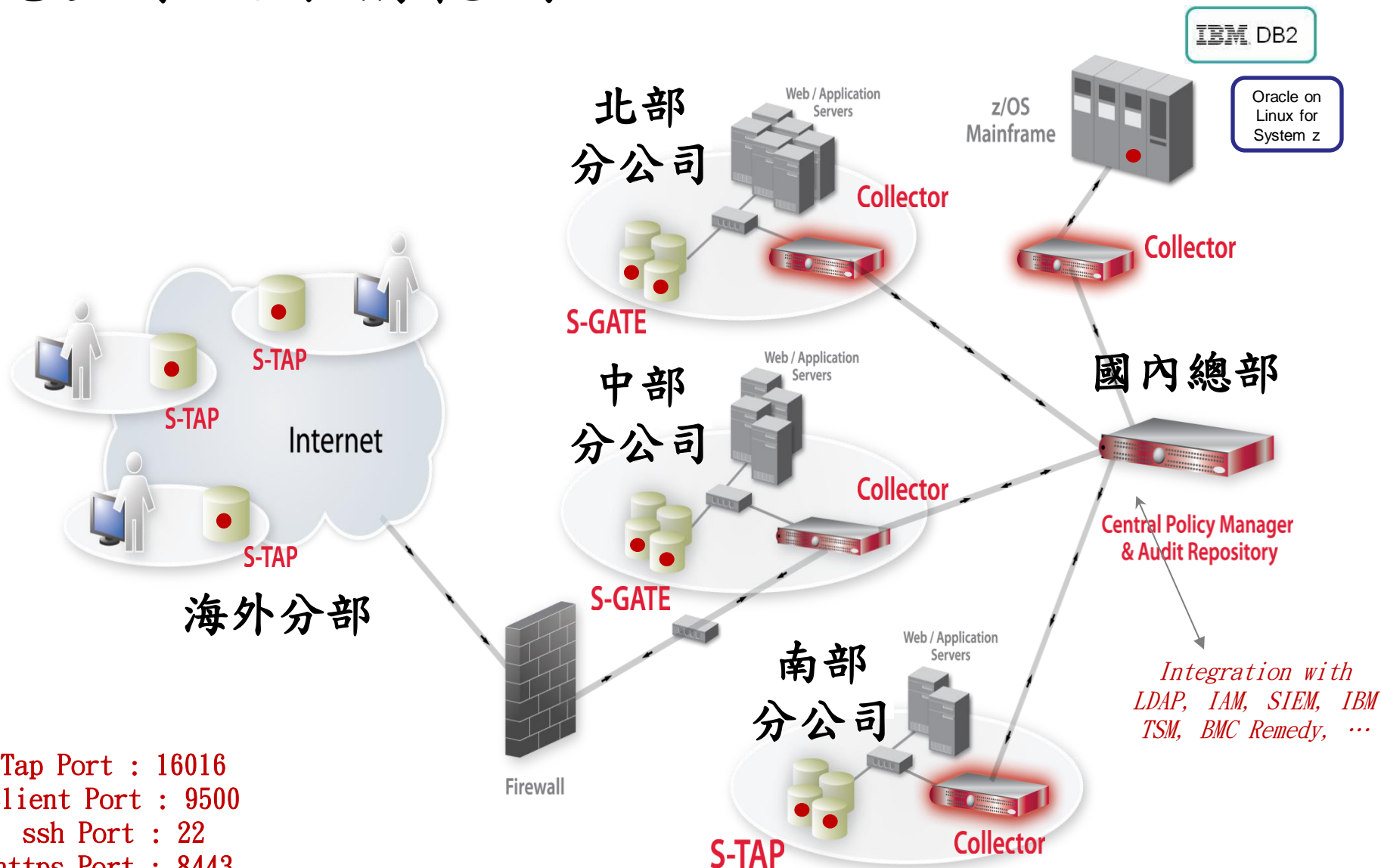


# 資料集中化管理





# 完整系統架構範例



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

*Integration with  
 LDAP, IAM, SIEM, IBM  
 TSM, BMC Remedy, ...*



# 稽核資料中長期保存

Administration Console

**Configuration Setup**

- System
- Inspection Engines
- Policy Installation
- Portal Global Profile
- Application User Translation
- Alerter
- Anomaly Detection
- Session Inference
- IP-to-Hostname Aliasing
- Upload Key File
- Query Hint
- Incident Generation
- Flat Log Process
- Customer Uploads

**Data Management**

- Data Export
- Data Archive
- Results Archive
- Data Restore
- Archive Catalog
- Export
- Import
- CSV/CE
- System

**Central Management**

- Central Monitor
- Local Taps
- S-Tap Configuration
- CAS Status
- SSH Public Key
- Guardium Installation
- Export Import

**Data Archive Configuration:**

Archive data older than:  Day(s)

Ignore data older than:  Day(s) (optional)

Archive Values

EMC CENTERA

TSM

SCP

Host:

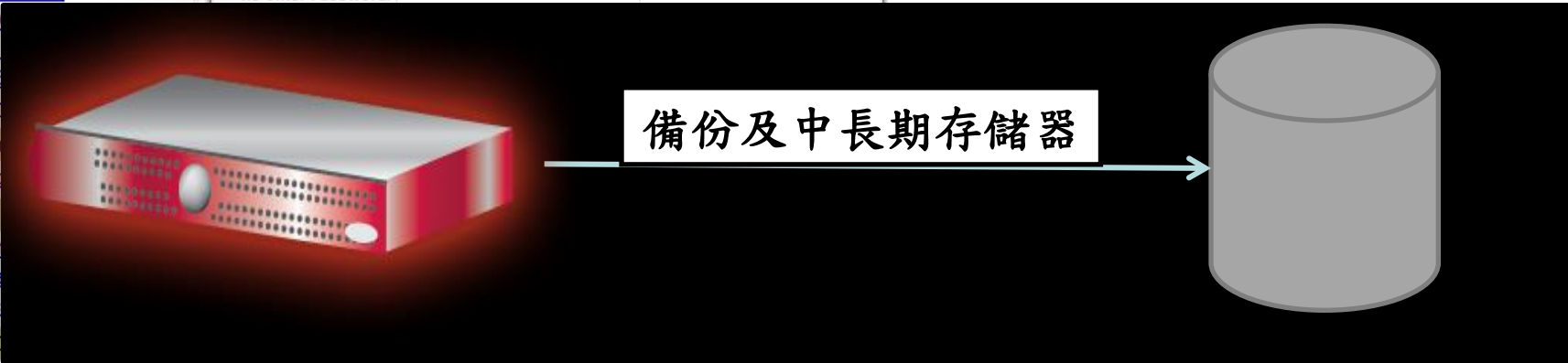
Directory:

SCP/FTP Username:

Password:

Re-enter Password:

```
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

