



IBM Software Group

Smarter Software for Smarter World

Jason Chuang

IBM SWG Taiwan

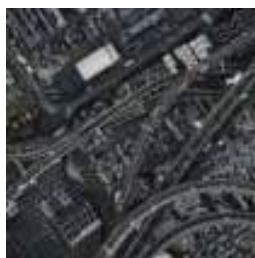


ON DEMAND BUSINESS™

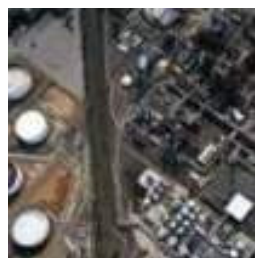
© IBM Corporation

The world is getting smarter

More instrumented, interconnected, intelligent



Smart traffic systems



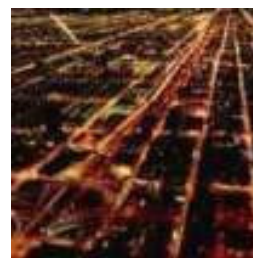
Intelligent oil field technologies



Smart food systems



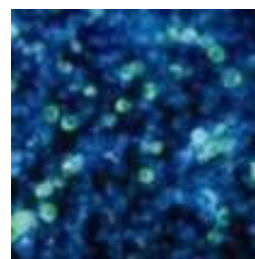
Smart healthcare



Smart energy grids



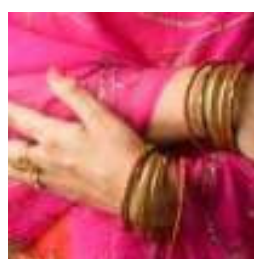
Smart retail



Smart water management



Smart supply chains



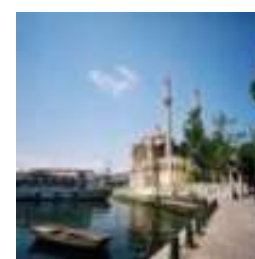
Smart countries



Smart weather

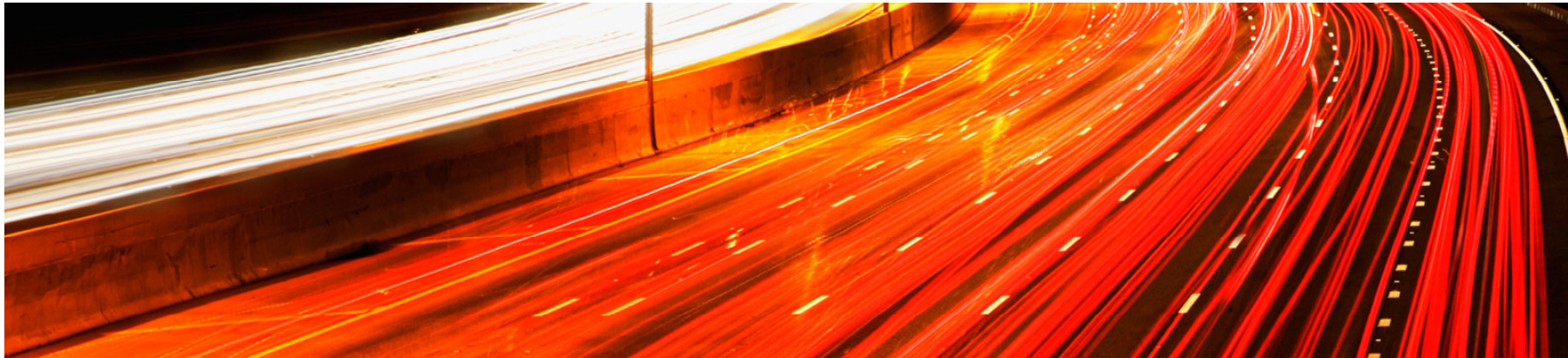


Smart regions



Smart cities

Think about the workloads that enable intelligent traffic systems ...



Electronic Toll Collection

Transaction processing systems (OLTP) linked to bank accounts and credit cards needing high integrity and availability

Traffic Flow Prediction

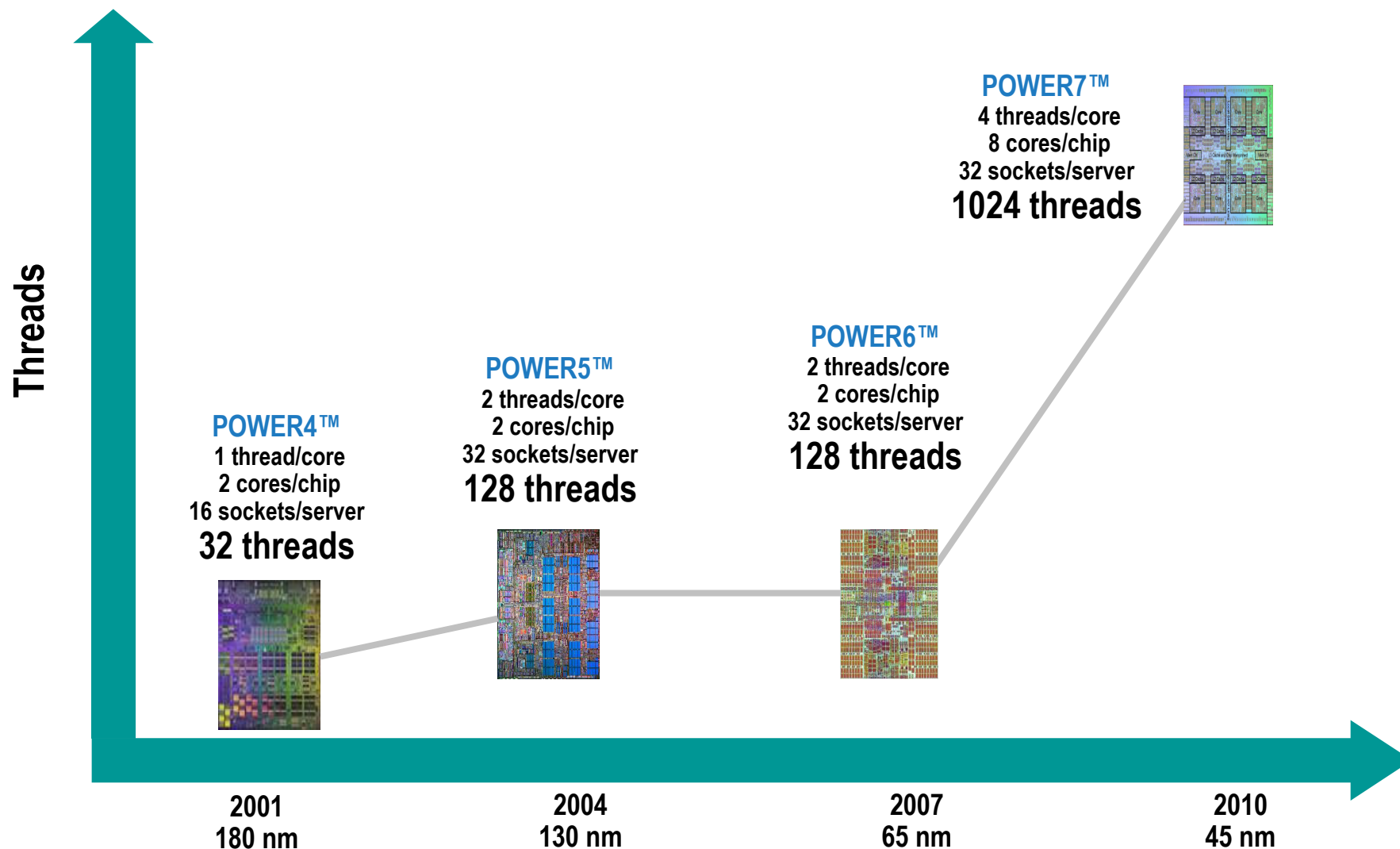
Analytic workload system looking for patterns in large volume of real-time and historical data

Weather, Local News, Major Events and Other Relevant Informational sources

Integrate processes and people in an agile fashion

Smarter Planet solutions have diverse workloads

Hardware system is get more POWERful



Smarter software running on powerful machine

No Brute Force



IBM Software Group

A Technical Introduction to DB2 pureScale

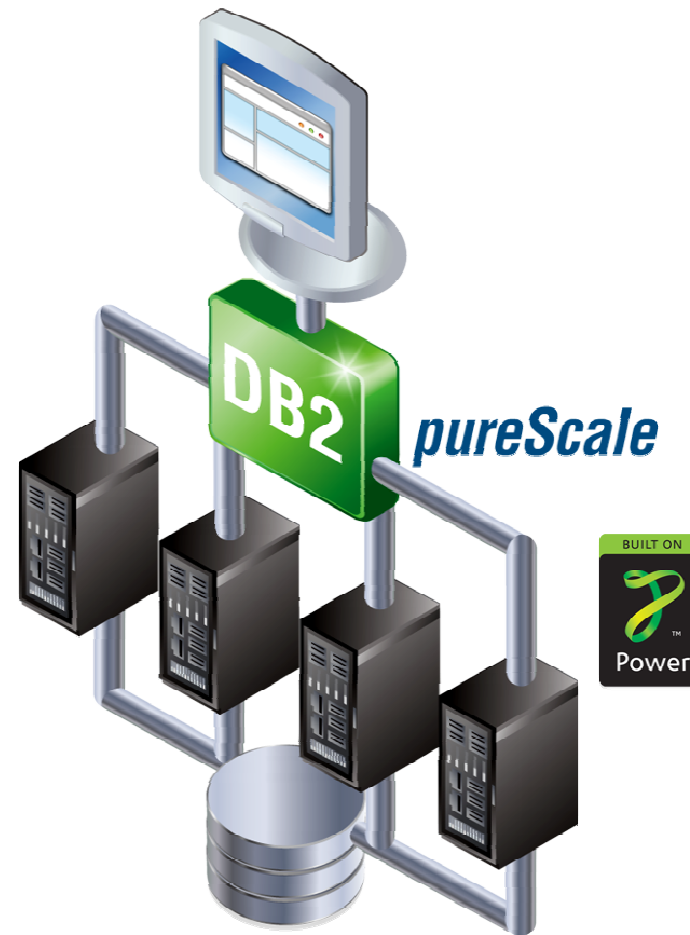
A horizontal decorative bar containing a series of small, square icons. From left to right, the icons include: a green square, a yellow square, a red square, a purple square, a cyan square, a grayscale image of a building, a circular arrow icon, a grayscale image of a woman's face, a grayscale image of a hand holding a device, and several grayscale squares of varying shades.

ON DEMAND BUSINESS™

© IBM Corporation

Customers' needs for 24x7 OLTP system

- High Availability
- Linear scale-out capability
- Load balances
- Application Transparent



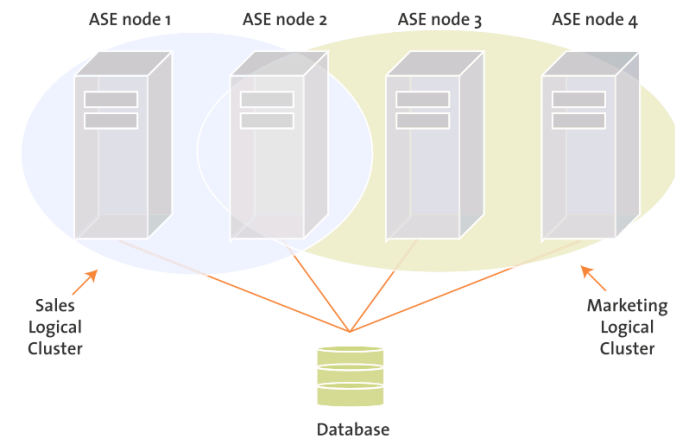
What were available on the market?

- Key technology (and problems)
 - ▶ Data Mastering
 - Each data block mastered by one node
 - ▶ Cache Fusion
 - ▶ Global Lock Manager
 - ▶ Heavy communication between DB nodes
 - Bad scalability ($1 + 1 \ll 2$)
 - ▶ Application Partitioning to increase scalability
 - NOT Application transparent
 - ▶ Data Re-mastering during fail over
 - System freeze, NOT zero-downtime

Oracle RAC

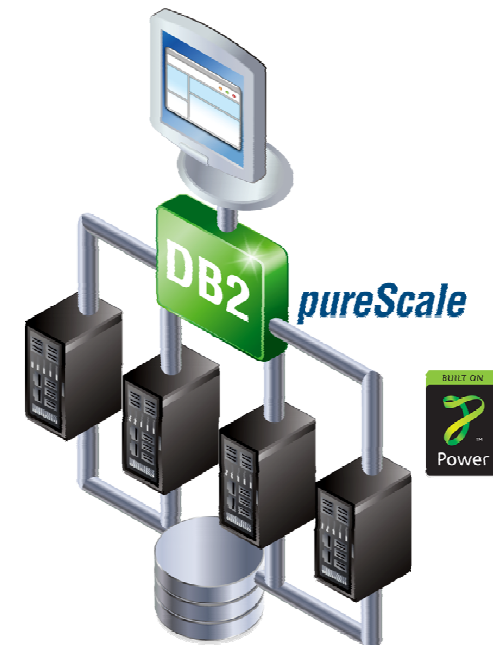


Sybase Cluster

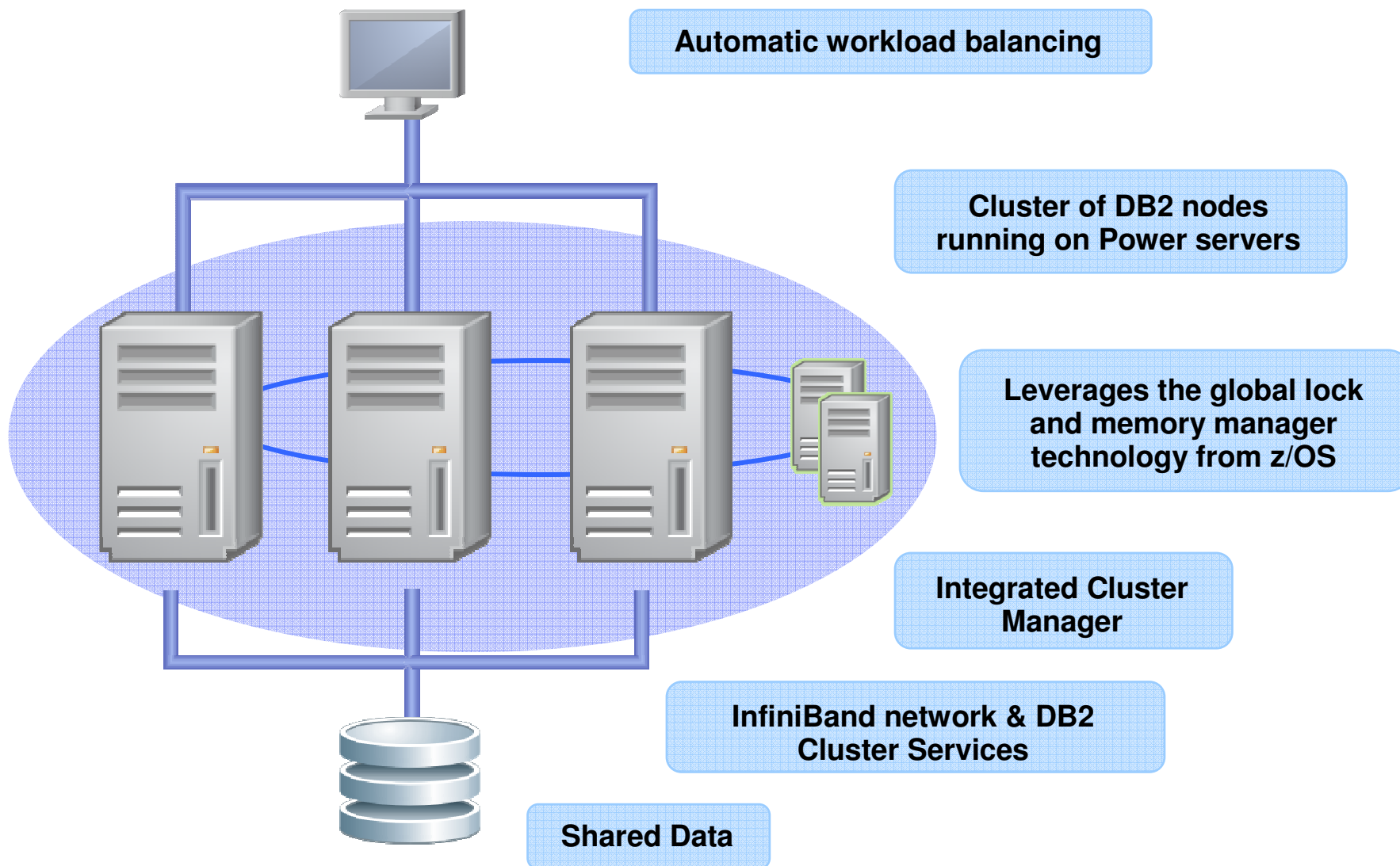


Where does DB2 PureScale come from?

- Everyone recognizes DB2 for z/OS as the “Gold” standard for scalability and high availability
- Why?
 - ▶ The Coupling Facility!!
 - Centralized locking, centralized buffer pool deliver superior scalability and superior availability
 - ▶ The entire environment on z/OS uses the Coupling Facility
 - CICS, MQ, IMS, Workload Management, and more



DB2 pureScale Architecture



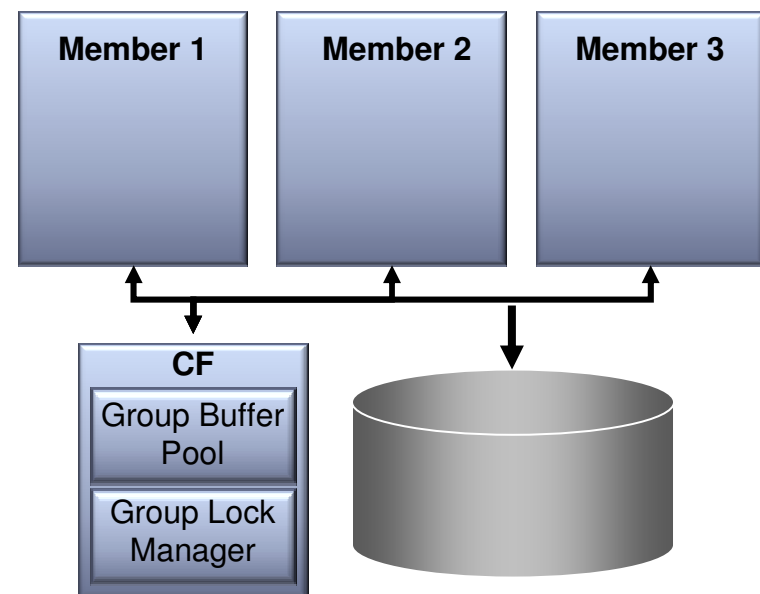
Key Technologies and benefits

- **Centralized Locking and Caching**

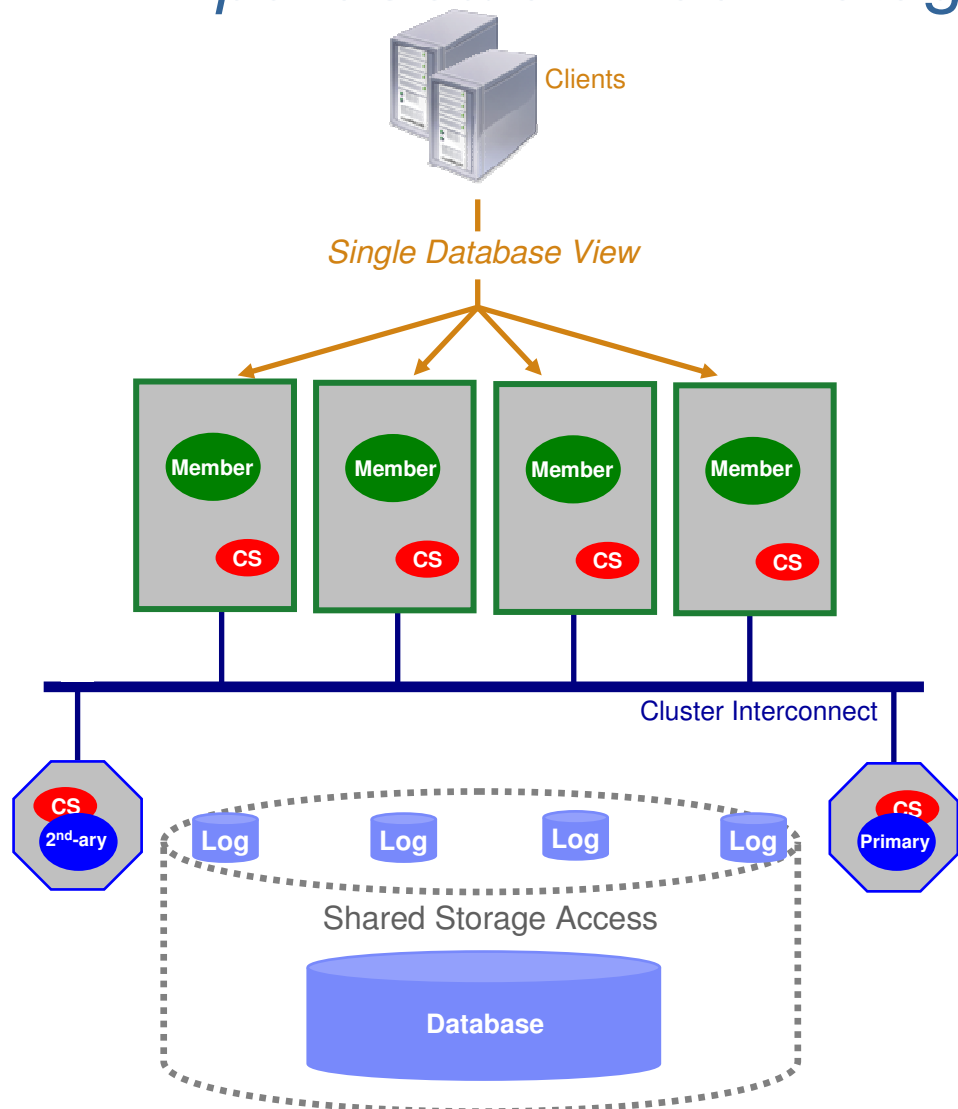
- ▶ As the cluster grows, DB2 maintains one place to go for locking information and shared pages
- ▶ Optimized for very high speed access
 - DB2 pureScale uses **Remote Direct Memory Access** (RDMA) to communicate with the powerHA pureScale server
 - No IP socket calls, no interrupts, no context switching

- **Results**

- ▶ Near Linear Scalability (1 + 1 => 2)
- ▶ Constant awareness of what each member is doing
 - If one member fails, no need to block I/O from other members
 - Recovery runs at memory speeds



DB2 pureScale : Technology Overview



Clients connect anywhere, see single database

- ▶ Clients connect into any member
- ▶ Automatic load balancing and client reroute may change underlying physical member to which client is connected

DB2 engine runs on several host computers

- ▶ Co-operate with each other to provide coherent access to the database from any member

Integrated cluster services

- ▶ Failure detection, recovery automation, cluster file system
- ▶ In partnership with STG and Tivoli

Low latency, high speed interconnect

- ▶ Special optimizations provide significant advantages on RDMA-capable interconnects (eg. Infiniband)

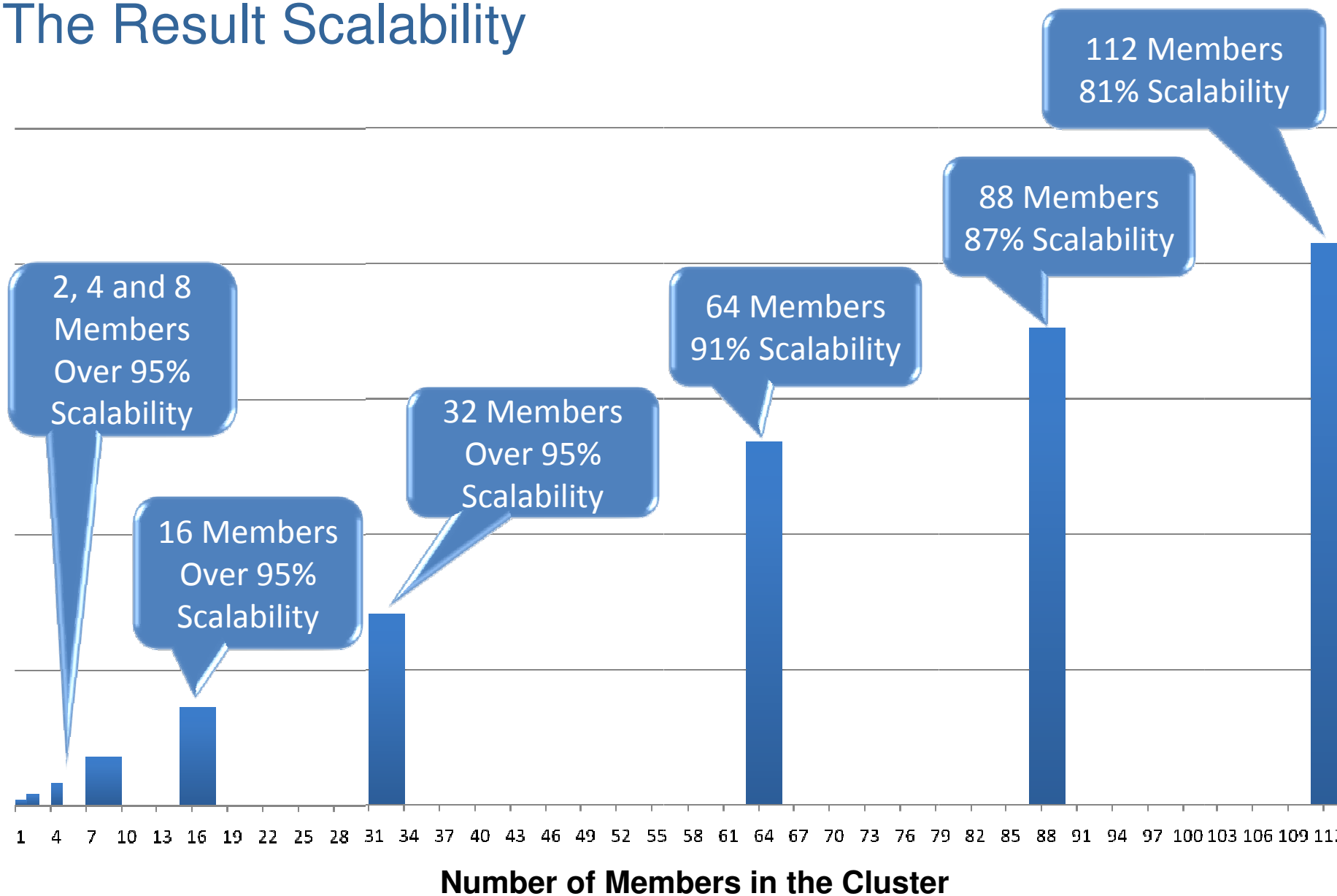
PowerHA pureScale technology

- ▶ Efficient global locking and buffer management
- ▶ Synchronous duplexing to secondary ensures availability

Data sharing architecture

- ▶ Shared access to database
- ▶ Members write to their own logs
- ▶ Logs accessible from another host (used during recovery)

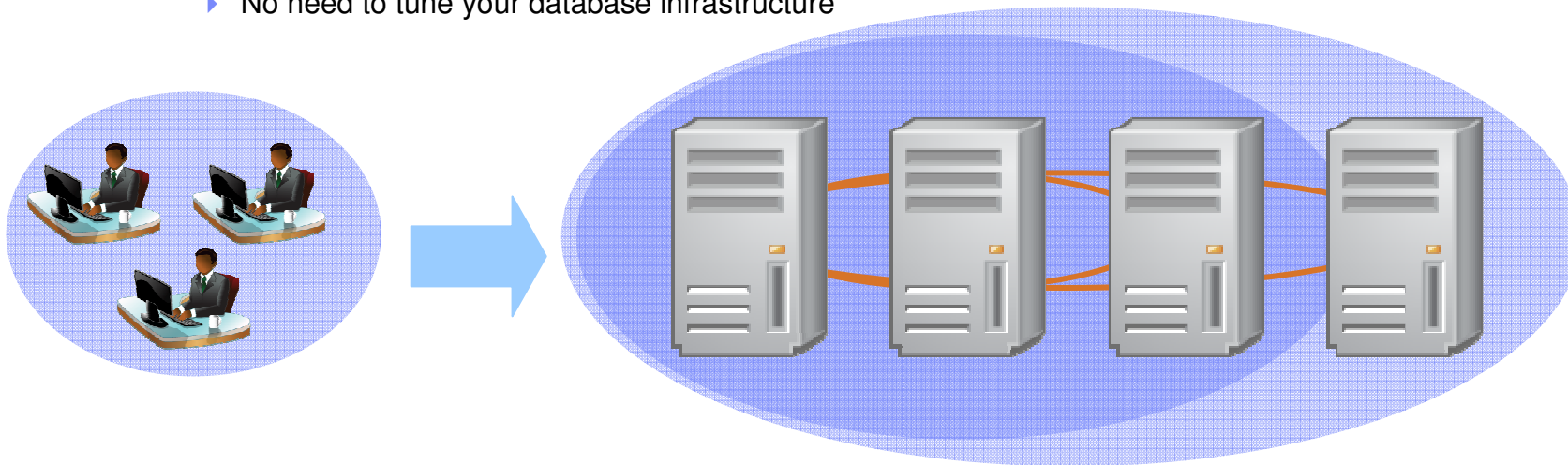
The Result Scalability



Application Transparency

Take advantage of extra capacity instantly

- ▶ No need to modify your application code
- ▶ No need to tune your database infrastructure

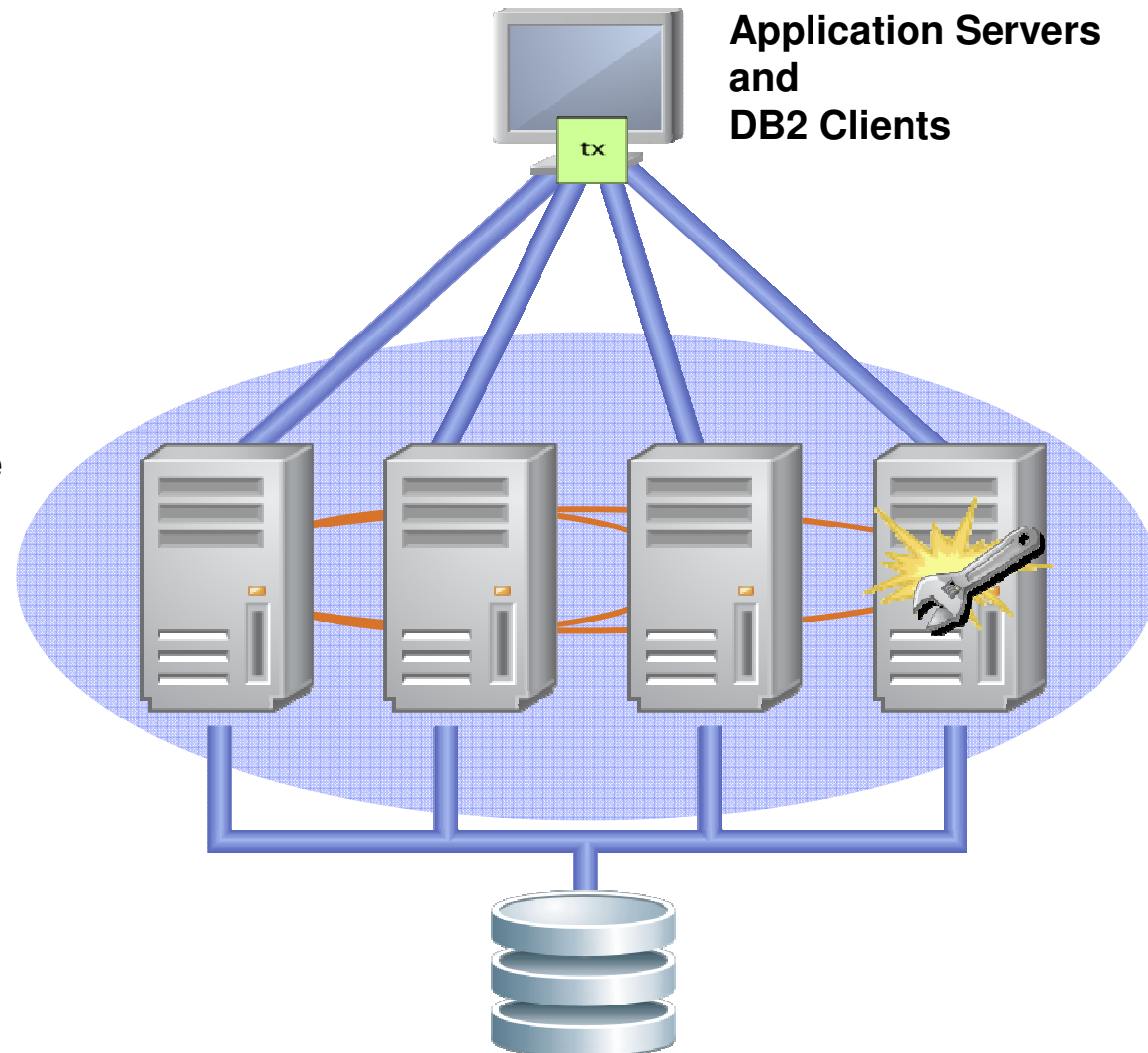


Your DBAs can add capacity without re-tuning or re-testing

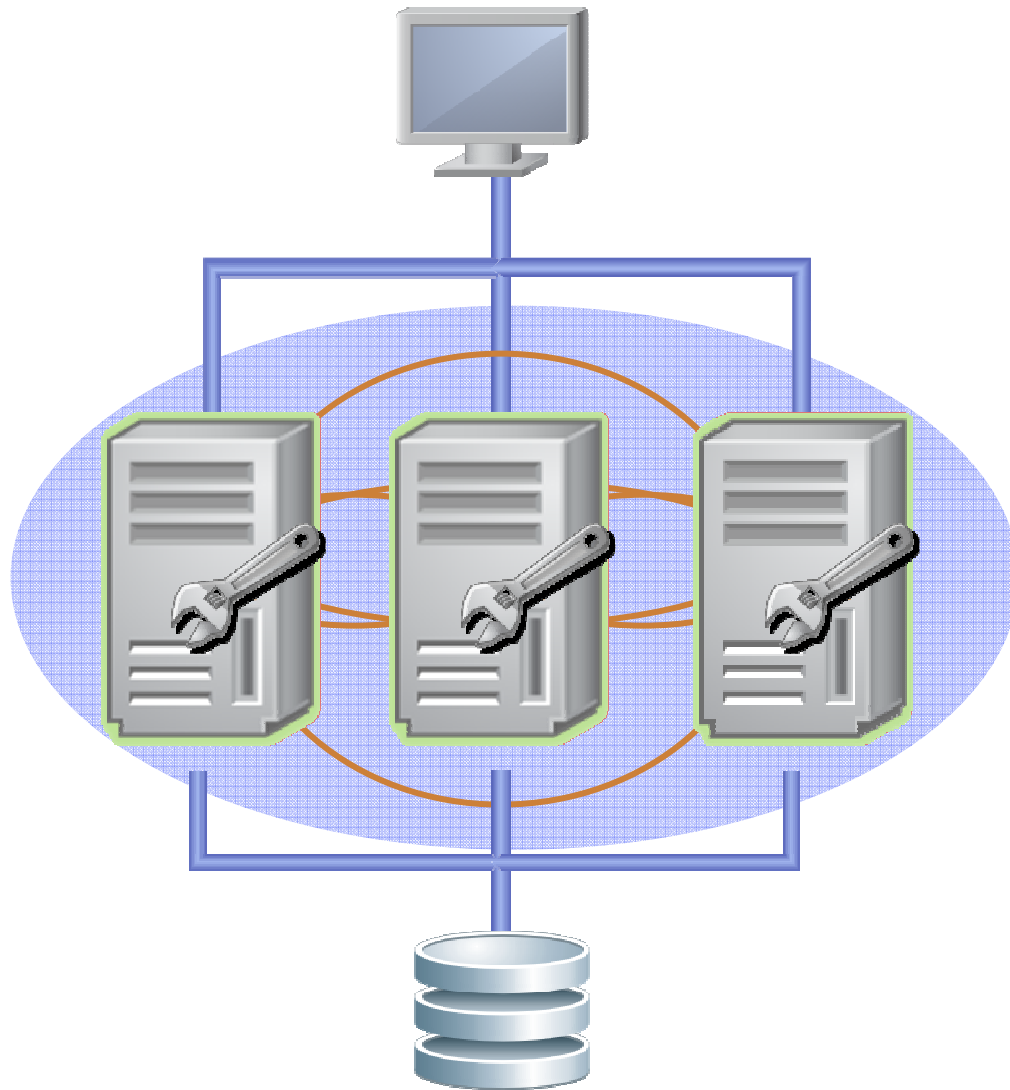
Your developers don't even need to know more nodes are being added

Recover Instantaneously From Node Failure

- Protect from infrastructure related outages
 - ▶ Redistribute workload to surviving nodes immediately
 - ▶ Completely redundant architecture
 - ▶ Recover in-flight transactions on failing node in as little as 15 seconds including detection of the problem



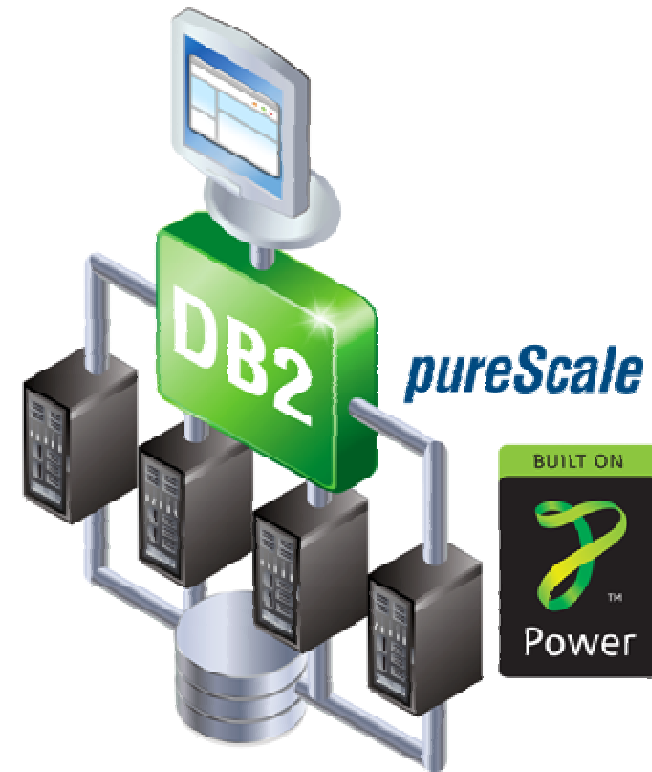
Minimize the Impact of Planned Outages



- Keep your system up
 - ▶ During OS fixes
 - ▶ HW updates
 - ▶ Administration

DB2 pureScale

- Unlimited Capacity
 - ▶ Buy only what you need, add capacity as your needs grow
- Application Transparency
 - ▶ Avoid the risk and cost of application changes
- Continuous Availability
 - ▶ Deliver uninterrupted access to your data with consistent performance



Learn how DB2 pureScale can help you reduce the risk and cost of meeting changing business demands



IBM Software Group

Guardium - IBM Database Auditing and Security Solution

A horizontal banner with a series of small, square icons in various colors (green, yellow, red, purple, cyan) and grayscale images (a person's face, a hand holding a device, a globe, etc.) on a gray background.

ON DEMAND BUSINESS™

© IBM Corporation

個資外洩問題不斷，並顯示內部人員問題和外界的入侵同等嚴重

出賣考生個資 博暉判賠349萬

*Source: 聯合報

【聯合報／記者呂開端 B106／桃園報導】

2009.06.07 02:29 am

台中市博暉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暉訴請每洩漏一人罰100元的懲罰性賠償，桃園地院昨天判博暉應賠償349萬餘元。

桃園地院調查，博暉公司標到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數加密電子檔等，還與主辦的國立桃園高級中學簽定「**盜賣資料**」的契約。

桃園法院指出，博暉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。

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「東森購物流出身分證字號等一應俱全」的檔案，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。

*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刪除，但老師們擔心，會讓有心人惡意使用。幾天前在中國的入口網站，由縣的100多位認輔教師的個人資料，全都一覽無遺，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

自由時報 電子報
The Liberty Times 生活新聞

自由新聞 影音娛樂 讀者園地 旅遊玩樂 好康報報 TAPEI TIMES Blog 新聞

今日要聞
PayEasy受「駭」 5400會員個資外洩
系統入侵

購物網站PayEasy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

*Source: 自由時報

2009-3-21

4校長涉賣10萬學生個資

與補習班勾結 中彰廿多校受害

〔彰化小組／綜合報導〕校長為錢，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資料，**盜賣資料**。據悉，該市有二十多所學校的資料被「賣」。

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，為免吳芝庭串證或湮滅證據，將她收押至今。

您的企業是否常面臨到下面問題

- Internal threats
 - ▶ Identify unauthorized changes
 - ▶ Prevent data leakage
- External threats
 - ▶ Prevent theft
- Compliance
 - ▶ Simplify processes
 - ▶ Reduce costs



Enterprise Database Security and Monitoring

- Who is changing database schemas or dropping tables?
- When are there any unauthorized source programs changing data?
- What are DBAs or outsourced staff doing to the databases?
- How many failed login attempts have occurred?
- Who is extracting credit card data?
- What data is being accessed from which network node?
- What data is being accessed by which application?
- How is data being accessed?
- What are the access patterns based on time of day?
- What database errors are being generated?
- What is the exposure to sensitive objects?
- When is someone attempting an SQL injection attack?

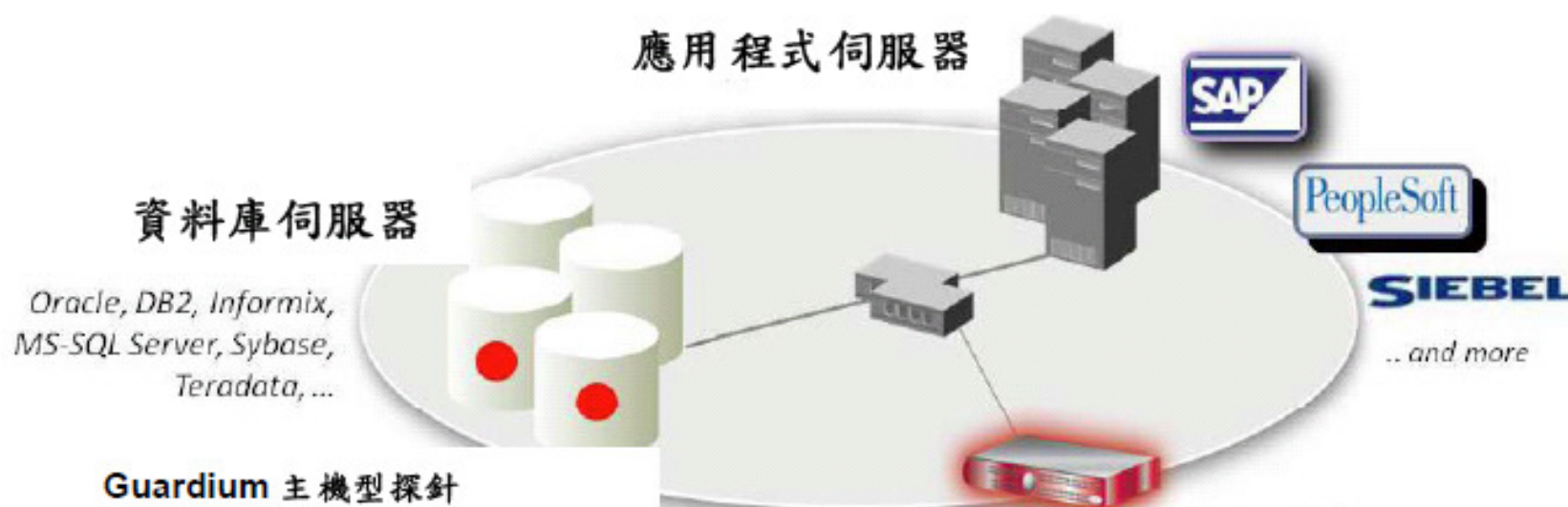
Why RDBMS's native audit does not work?

- 影響資料庫效能
- 非獨立作業-可以很容易被DBA關閉
- 不同廠牌資料庫稽核功能不一致
- 無法主動提供式即時安全警示
- 在 **Connection Pooling** 的環境無法確認應用程式端的使用者
- 須儲存大量稽核資料
- 須撰寫程式以篩選稽核資料時
- 須撰寫程式以產生稽核報表

Guardium 提供下列解決方案

- **Real-time database activity monitoring (DAM)**
 - ▶ 主動地偵測與發現出未經授權認可，或可疑的資料庫存取活動。
- **Auditing and compliance solutions**
 - ▶ 各項資料隱私安全處理方法的導入，能更簡易地符合各項法規，如SOX(美國沙賓法安 Sarbanes-Oxley)，PCI-DSS (支付卡產業資料安全標準 Payment Card Industry Data Security Standard)。
- **Change control solutions**
 - ▶ 預防未經授權者在資料庫結構上、資料數值、特定者使用權、及系統設定上作變更。
- **Vulnerability management solutions**
 - ▶ 在弱點安全控管上的判讀及解決方案。
- **Database leak prevention**
 - ▶ 找出敏感資料及資料庫造成威脅的安全缺口，並加以防護。

Guardium Solutions



Guardium 主機型探針

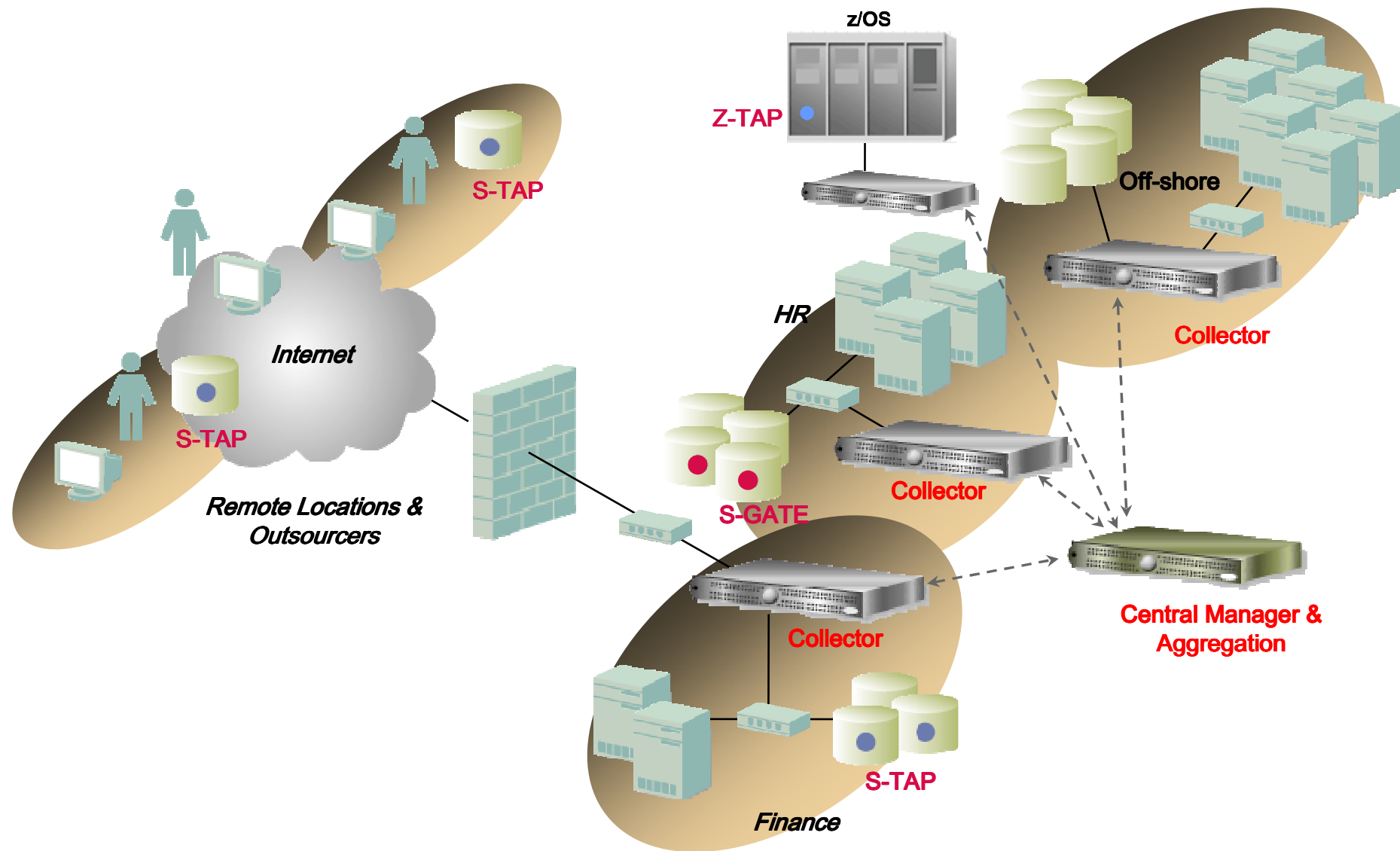
採用影響低的軟體探針，
監視各種資料庫活動
(包括特許使用者的活動)。
活動在作業系統核心層進行，
不需依賴原生審核日誌。

Guardium 收集器

提供即時、原則式監視、
分析、報告及審核資料儲存；
可用實體或虛擬應用方式處理。

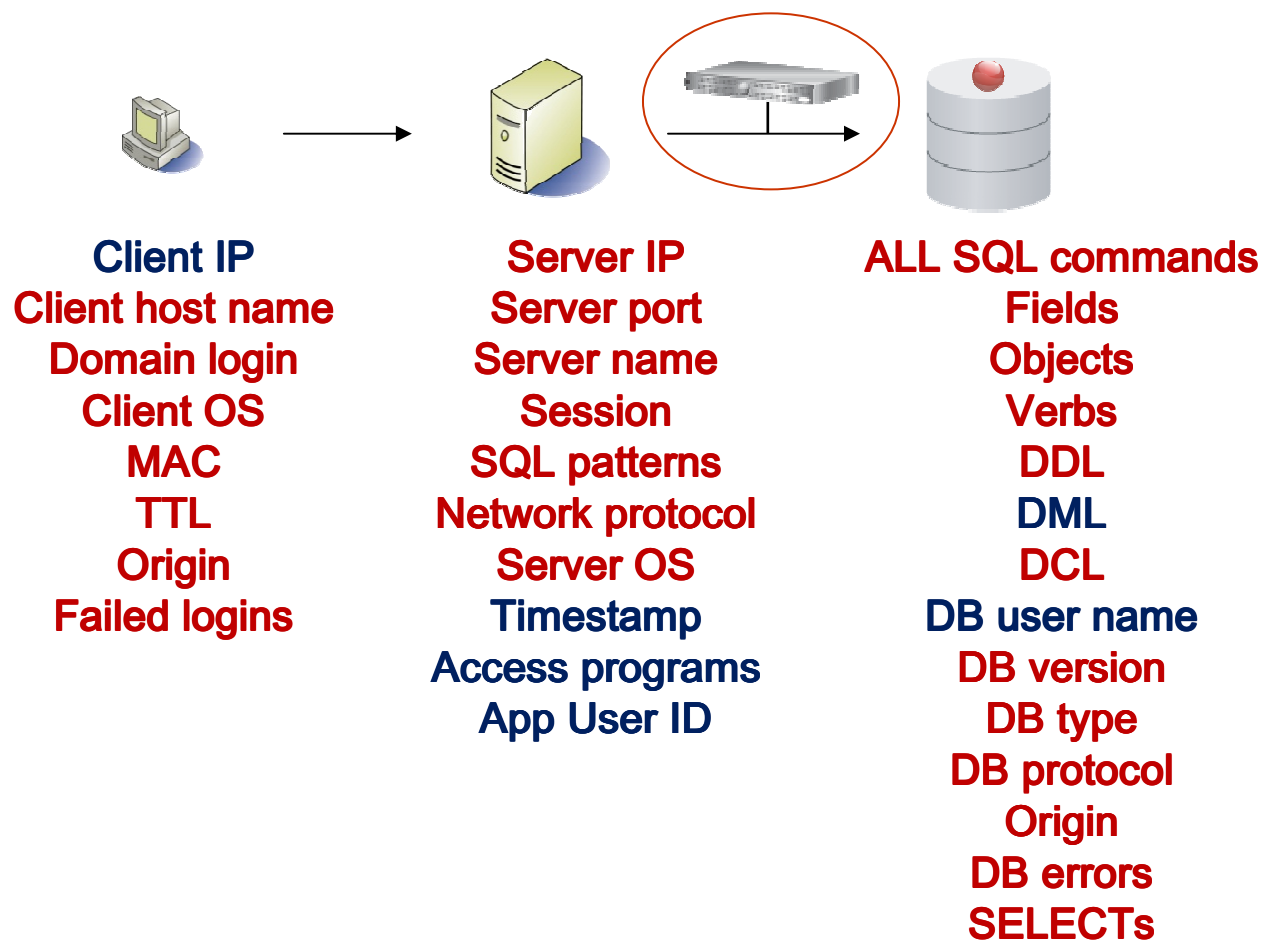
- 非侵入性
- DBMS獨立性
- 最小的系統影響
- 無需透過資料庫日誌和審計
- 細緻精密的策略與監控
- *Who, What, When, how, Where*
 - 即時警示
- 全面的活動監控包含本地端的存取

可擴展的多層次架構



詳盡的稽核項目




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





Security Policy - Sample Access Rule



- 紀錄針對Employee表格所下達的所有DML指令。

Policy Rules

Policy One Filter:   

Expand All Collapse All Select All Unselect All  Remove Selected  Copy Rules ...

1 Access Rule: Record values for employee DB DML cmds

Cat.	Classif.	Sev.	Client IP	Server IP	Src App.	DB Name	DB User	App. User	
ANY	ANY		ANY	ANY	ANY	ANY	ANY	ANY	
OS User	Service Name	Net. Protocol	Field Name	Pattern	XML Pattern	DB Type	Client MAC		
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	
Object	Command	Object/Command Group	Object/Field Group	Period	Min. Ct.	Reset Int.	Action	Rec. Vals.	Cont.
employee	DML Commands	ANY	ANY	ANY	0	0		<input type="checkbox"/>	<input checked="" type="checkbox"/>
App Event Exists	App Event Str. Val.	Event Type	App Event Num. VaL.	App Event Date	Event User Name				
<input type="checkbox"/>	ANY	ANY	ANY	ANY	ANY				

2 Exception Rule: Alert for SQL error on customer db

3 Extrusion Rule: Log suspected SSN output from EMP

Security Policy - Sample Exception Rule

- SQL指令產生錯誤訊息時，發出警訊並記錄所有資料。

Policy Rules

Policy One Filter: [-----] [v] [x] [?] [!]

Expand All Collapse All Select All Unselect All Remove Selected Copy Rules ...

1 Access Rule: Record values for employee DB DML cmds

2 Exception Rule: Alert for SQL error on customer db

Cat.	Classif.	Sev.	Client IP	Server IP	Src App.	DB Name	DB User	App. User
ANY	ANY	i	ANY	192.168.22.32 / 255.255.255.255	ANY	ANY	ANY	ANY
OS User	Service Name	Net. Protocol	DB Type	Client MAC				
ANY	ANY	ANY	ANY	ANY				
Exception Type	Error Code	Period	Min. Ct.	Reset Int.	Action	Rec. Vals.	Cont.	
SQL_ERROR	ANY	ANY	0	0	[Warning]	[x]	[]	[]

3 Extrusion Rule: Log suspected SSN output from EMP

Security Policy - Sample Extrusion Rule

- 當SQL查詢結果含有疑似身份證字號的資料時，紀錄所有詳細資訊。

Policy Rules

Policy One Filter: [-----] [v] [x] [?] [!]

Expand All Collapse All Select All Unselect All Remove Selected Copy Rules ...

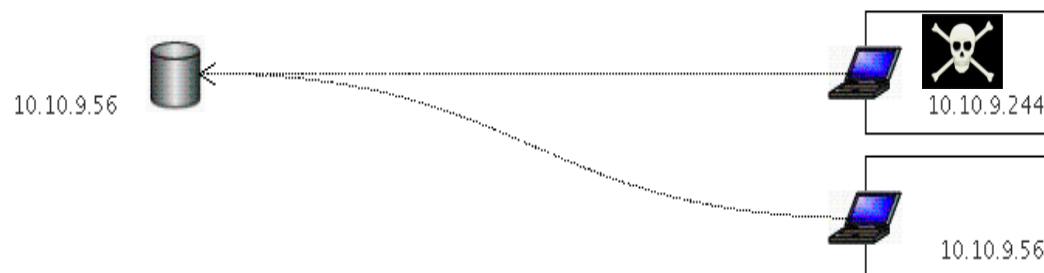
1 Access Rule: Record values for employee DB DML cmds

2 Exception Rule: Alert for SQL error on customer db

3 Extrusion Rule: Log suspected SSN output from EMP

Cat.	Classif.	Sev.	Client IP	Server IP	Src App.	DB Name	DB User	App. User
ANY	ANY	i	ANY	192.168.22.37 / 255.255.255.255	ANY	EMPLOYEE_INFO	ANY	ANY
OS User	Service Name	Net. Protocol	DB Type	Client MAC				
ANY	ANY	ANY	ANY	ANY				
Data Pattern	Masking Pattern	Sql Pattern	Period	Min. Ct.	Reset Int.	Action	Rec. Vals.	Revoke
[0-9]{3}-[0-9]{2}-[0-9]{4}	ANY	ANY	ANY	0	0	Log	<input type="checkbox"/>	<input type="checkbox"/>

Policy Exception Rule - Preventing Attacks



Rogue users know what they're looking for, but...

They don't always know where to find it!

Returned SQL Errors

Start Date: 2007-03-01 00:00:00 End Date: 2007-04-15 00:00:00

Client IP	Server IP	Server Type	DB User Name	Database Error Text
10.10.9.244	10.10.9.56	ORACLE	APPLSYSUB	ORA-00942: table or view does not exist

SQL injection leads to **SQL errors!**

Failed Login Attempts

Start Date: 2007-03-01 00:00:00 End Date: 2007-05-01 00:00:00

User Name	Source Address	Destination Address	Database
MarcG	192.168.20.107	10.10.9.56	ORACLE
APPLSYSUB	10.10.9.244	10.10.9.56	ORACLE
APPLSYSUB	10.10.9.56	10.10.9.56	ORACLE

Brute force attacks result in **failed logins!**

Guardium: 100% visibility with real-time alerts ...

弱點偵測

- Evaluate your system's security strength and compare with industry best practices
 - ▶ Computer Internet Security (CIS), Security Technical Implementation Guide (STIG), ..
- Broad range of probings/testings
 - ▶ Privileges
 - Object usage rights, Privilege grants to DBAs and users, ..
 - ▶ Authentications
 - Password policies, empty password, remote login parameters, ..
 - ▶ Configuration
 - Max failed login, not allow system table updates, SYSADM_GROUPS, ..
 - ▶ Behavior
 - Excessive after-hours logins, login failures, execution of privilege commands, ..
 - ▶ File permission
 - DB home directories, configuration files, registry/environment variables, ..

Vulnerability Assessment Example

Guardium

Results for Security Assessment: **Comprehensive Oracle Assessment**

Assessment executed 2009-08-21 12:47:28.0

From: 2009-08-20 12:47:28.0 To: 2009-08-21 12:47:28.0

Client IP or IP subnet: Any Server IP or IP subnet: Any

Download PDF

Overall Score

Tests passing: **42%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)
[Jump to Datasource list](#)

Detailed Scoring Matrix

Result Summary Showing 92 of 92 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	9p 15f	1p 4f	-- 1f	-- --	-- --
Authentication	2p 4f	-- 1f	-- 1f	-- --	-- --
Configuration	2p 2f	-- 8p 3f 4e	1p 3f 4e	-- 6f 1e	-- --
Version	-- --	-- 2f	-- --	-- --	-- --
Other	-- 2f	-- 2p 3f	-- 3p	-- 1e	-- -- 6p -- 1e

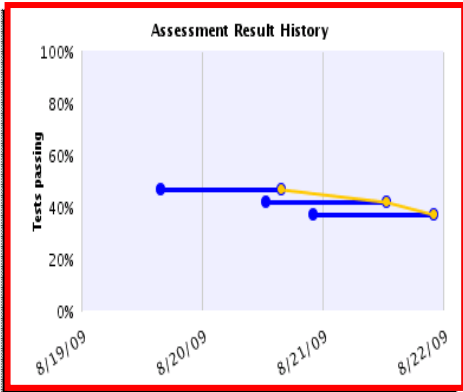
Current filtering applied:
Severities: - Show All -
Scores: - Show All -
Types: - Show All -

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results [Compare with Previous Results](#) Showing 92 of 92 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[Observed]	Fail	Critical	Too Many login failures, found 15 per day. <i>Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into your database, or of someone trying to steal or damage your data. The number of login failures should be close to zero, especially in production environments. You should immediately inspect all attempts to access your database and the source of all the login failures, and take immediate action to deny access to your database from unauthorized clients.</i>
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.59	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Historical Progress or Regression



Filter control for easy use

Show only: [Reset Filtering](#)

Severities	Scores	Test Types
Critical	Fail	SYBASE
Major	Pass	MS SQL SERVER
Minor	Error	INFORMIX
Cautionary		MYSQL

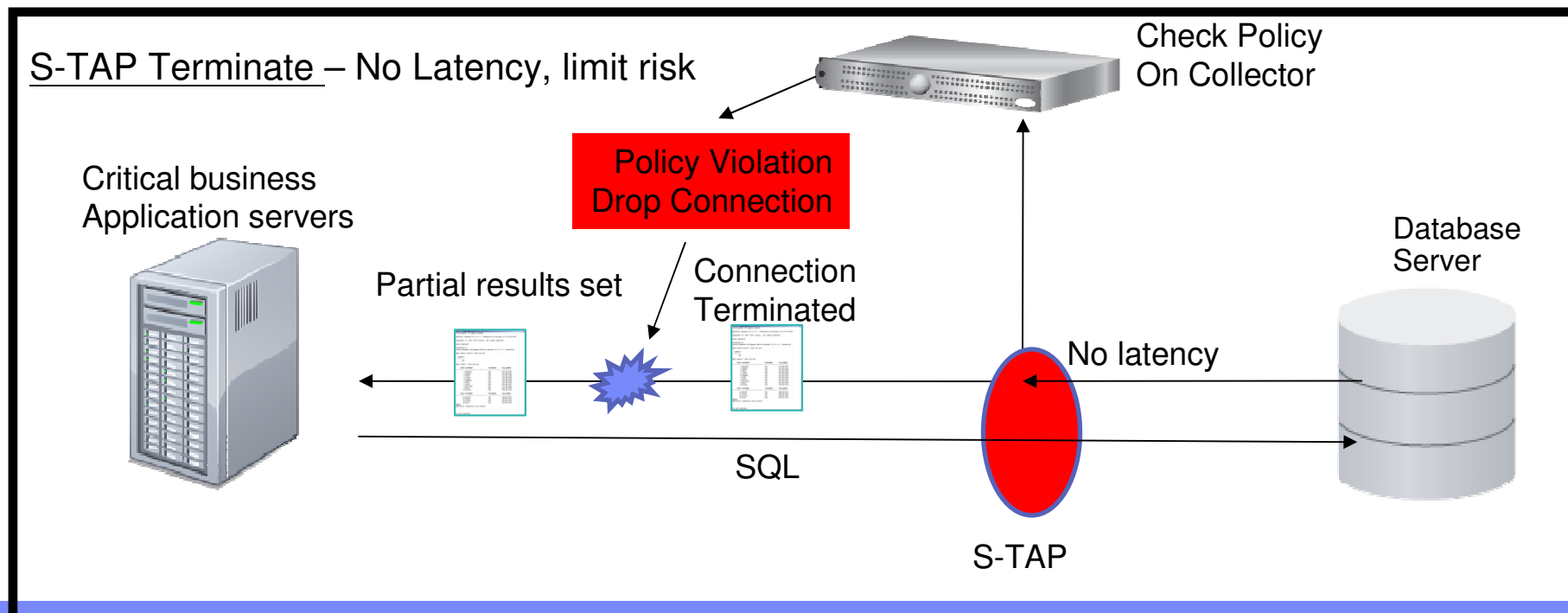
Sort by:

First	Second	Third
Severity	Score	Datasource

Apply

S-TAP Terminate principle

- Policy could terminate based on:
 - ▶ SQL command
 - Command will hit the database
 - ▶ Data Extrusion
 - Returned data/results set



S-Gate Terminate Overview

