從IBM資安架構看資料稽核與入侵防護

Eugene Liou
Software Client Architect, IBM Taiwan

大綱

- 現階段面臨的資安挑戰
- IBM資安架構
- 資料庫稽核解決方案
- 網路入侵防護解決方案

隨著行動裝置與社群網路的普及,敏感性的個人隱私資料逐漸擴散於企業所屬的各部門之間,如何防護敏感個資的外洩,已經成為企業的重要管理項目

DATA EXPLOSION

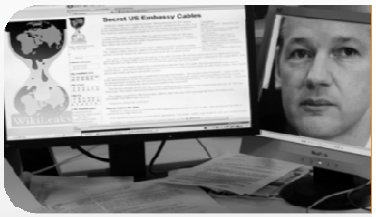
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

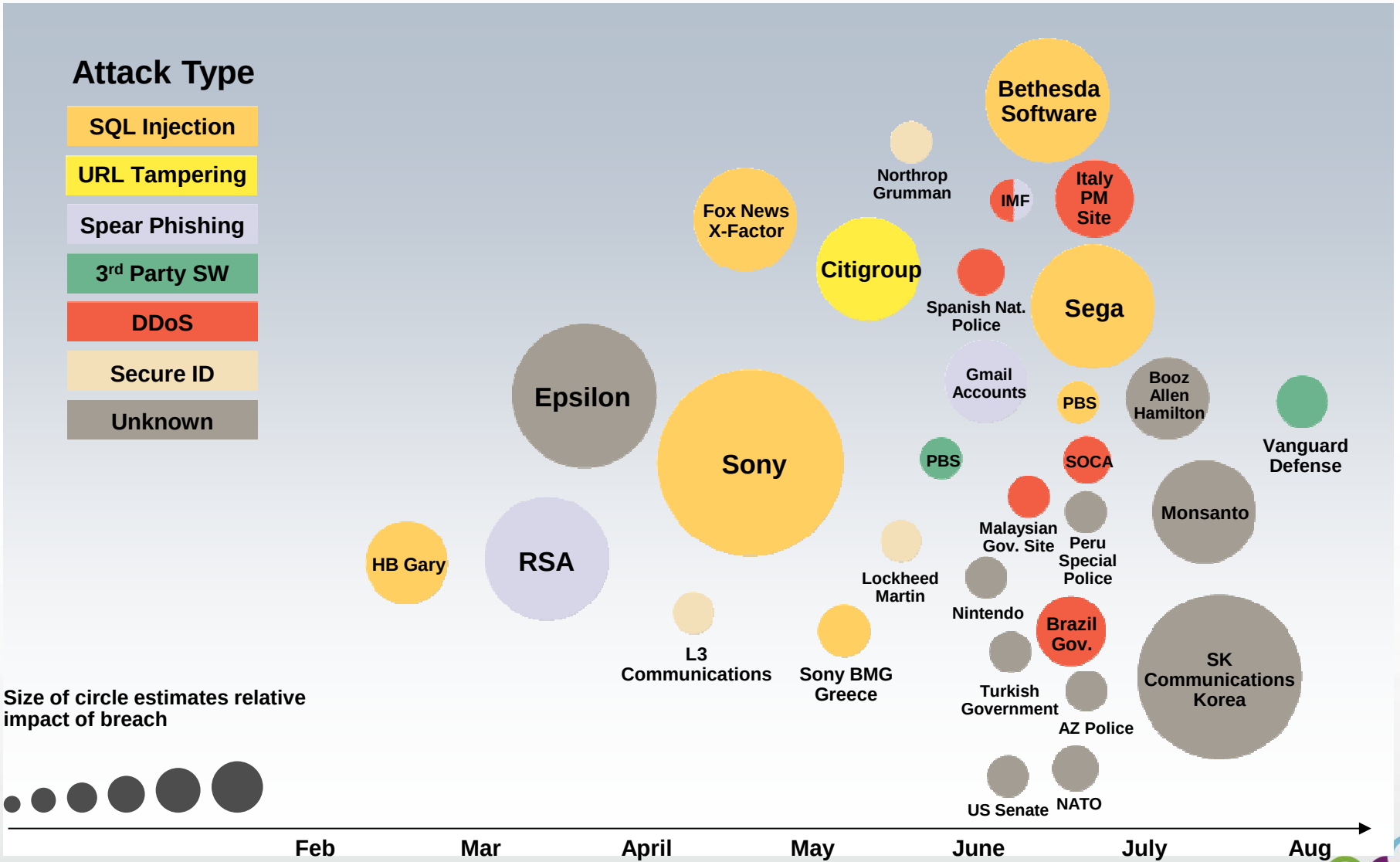
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

各式各樣的資安攻擊案例不斷衝擊企業的永續經營



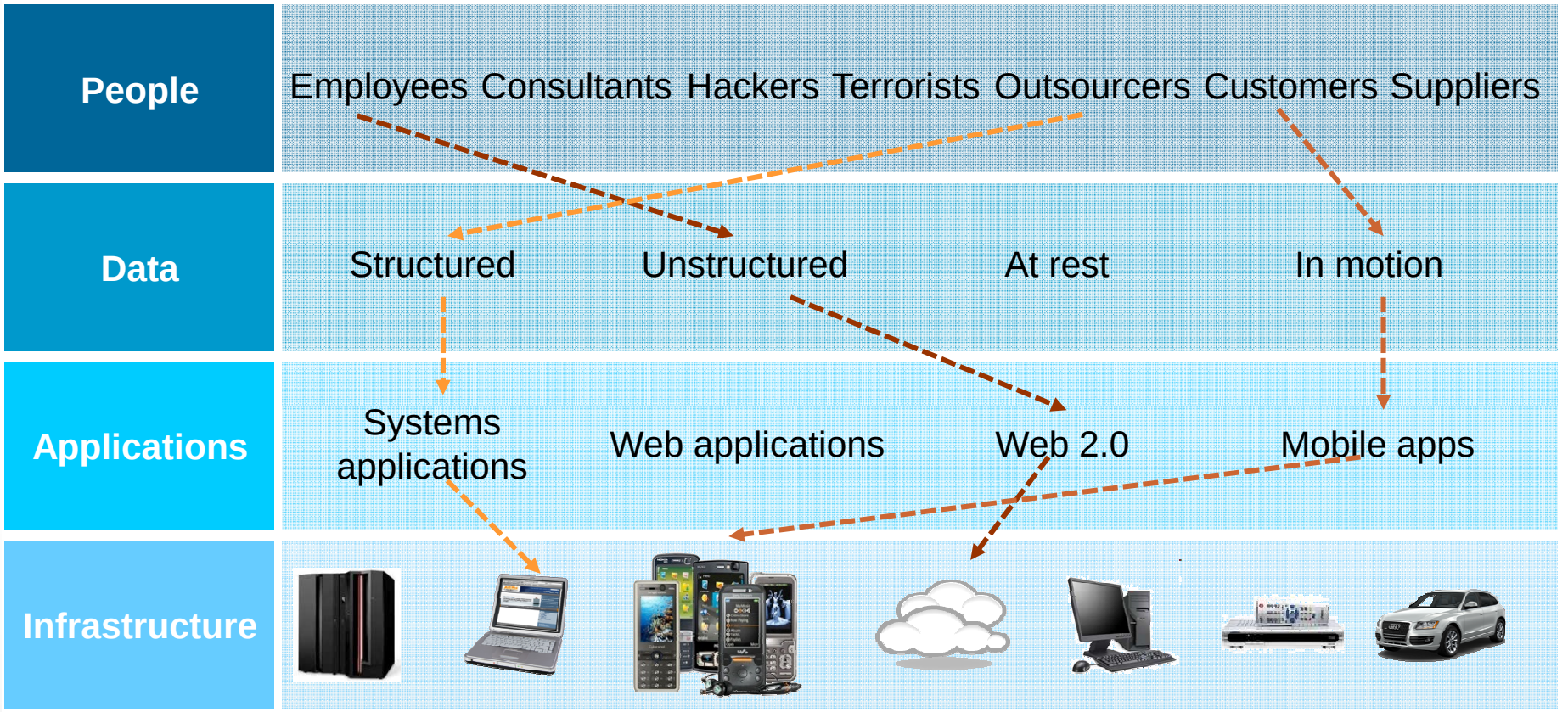
IBM Security X-Force® 2011 Midyear Trend and Risk Report September 2011

資訊安全已經成為企業經營決策者的重要討論議題

Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential $1B long term impact – $171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

*Sources for all breaches shown in speaker notes

解決資安問題相當複雜,我們建議應該從四個方向去思考

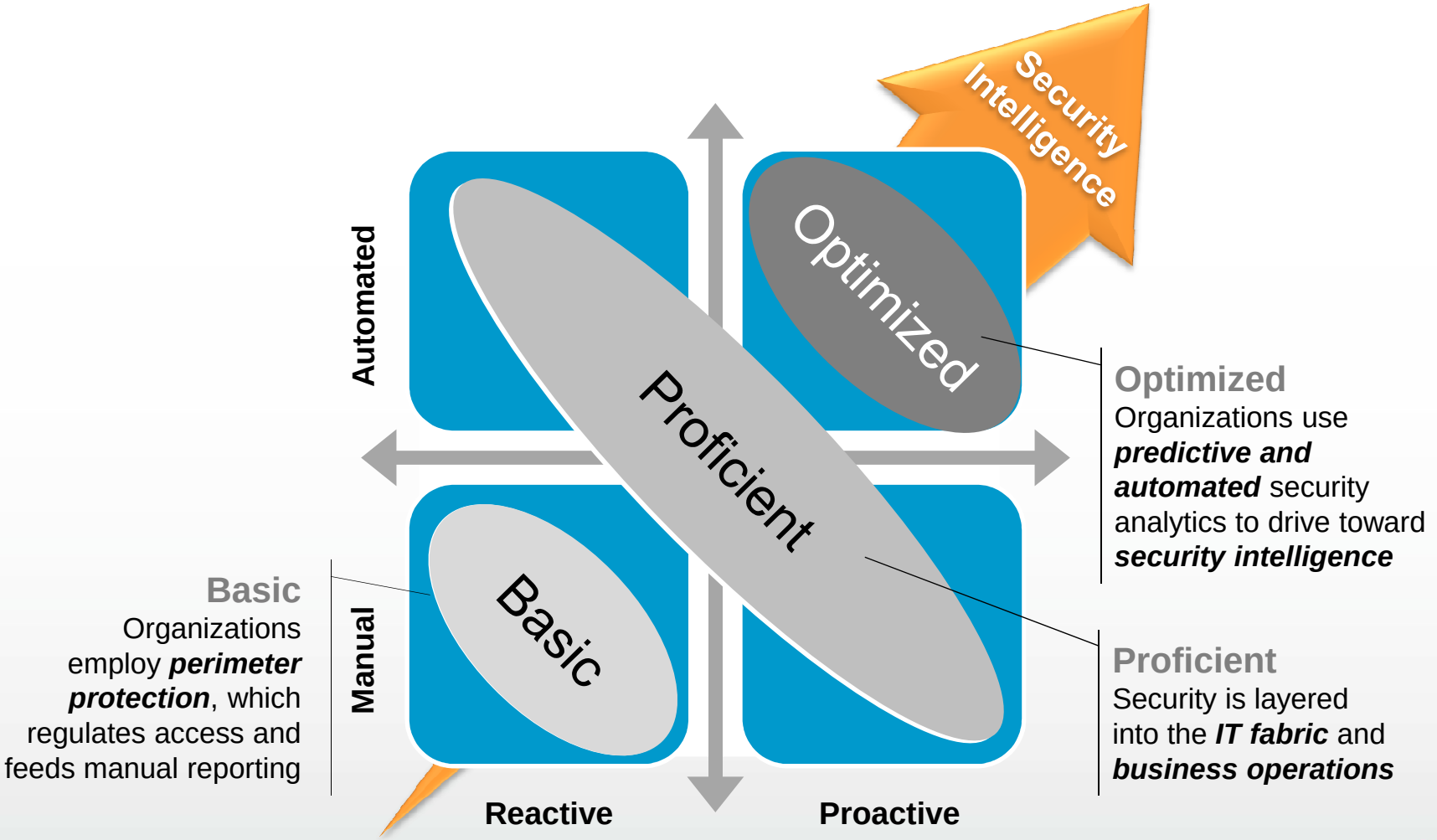


It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

大綱

- 現階段面臨的資安挑戰
- IBM資安架構
- 資料庫稽核解決方案
- 網路入侵防護解決方案

針對資安的解決方案也應該從基本的人工作業的被動方式升級成自動化作業的主動式智慧防護



Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

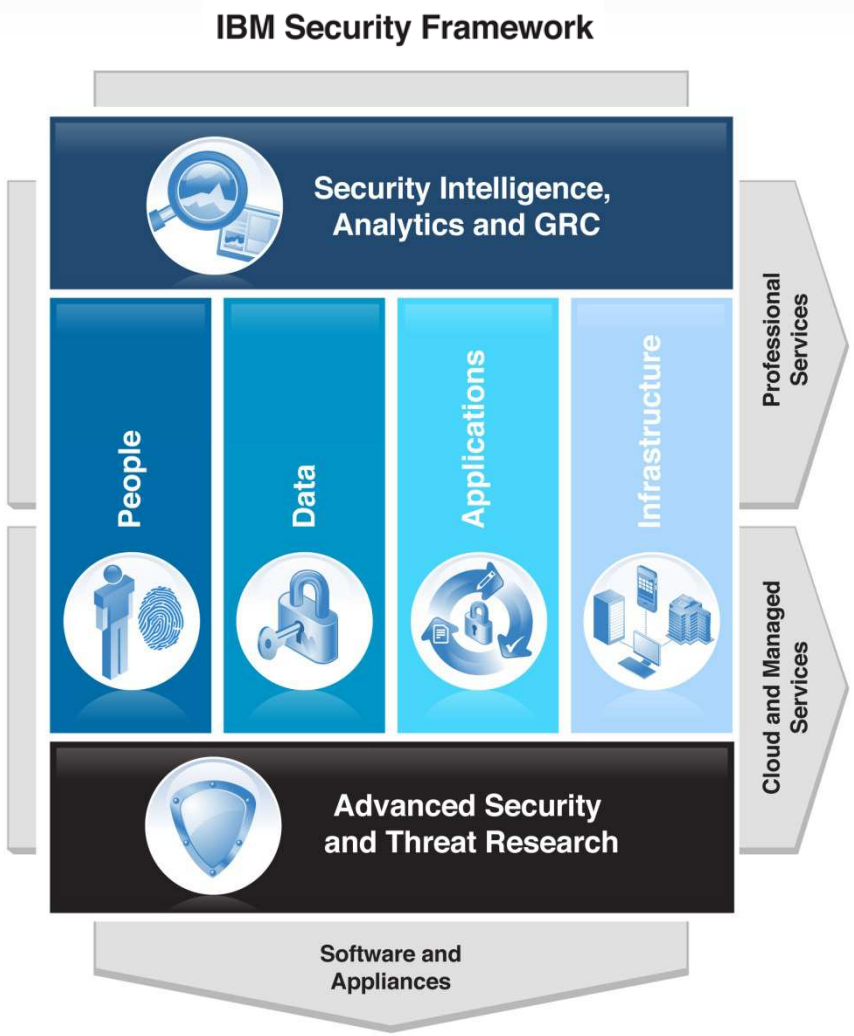
Proficient
Security is layered into the ***IT fabric*** and ***business operations***

因此除了前面所述的四個思考方向, IBM還提出了智慧,整合與專家管理等面向,來達成完整的資安架構

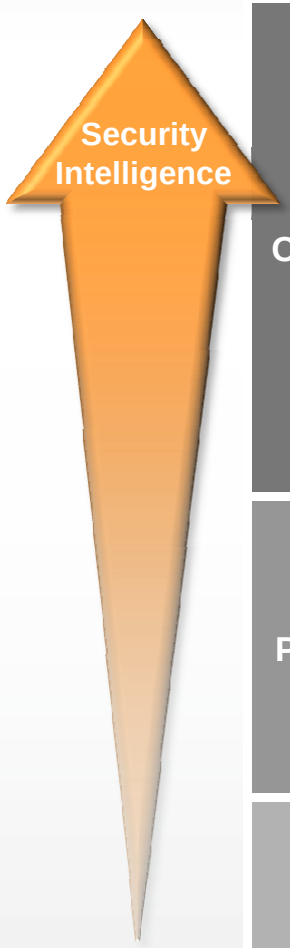
IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise

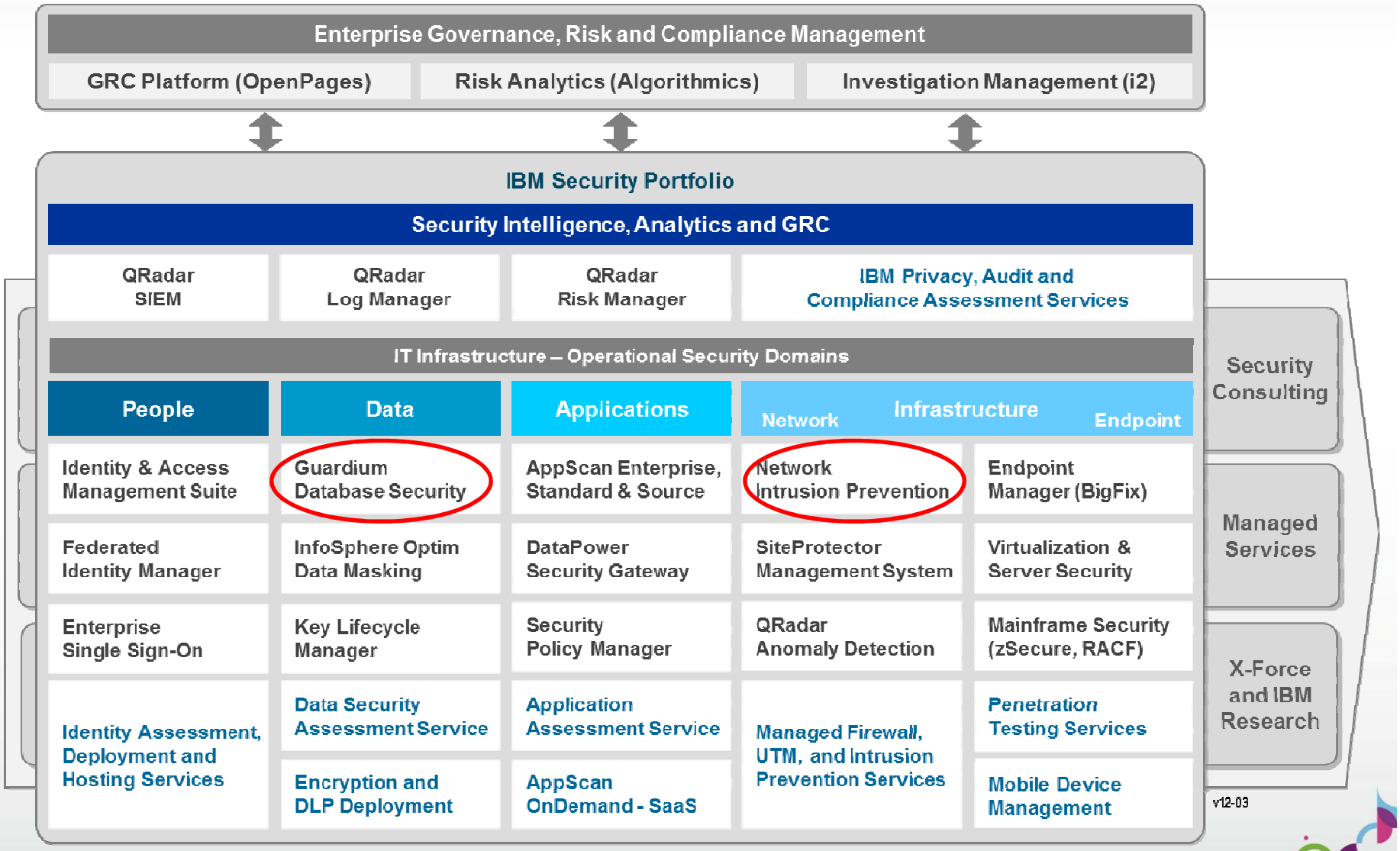


智慧型資安架構使企業的資安防護逐步的最佳化

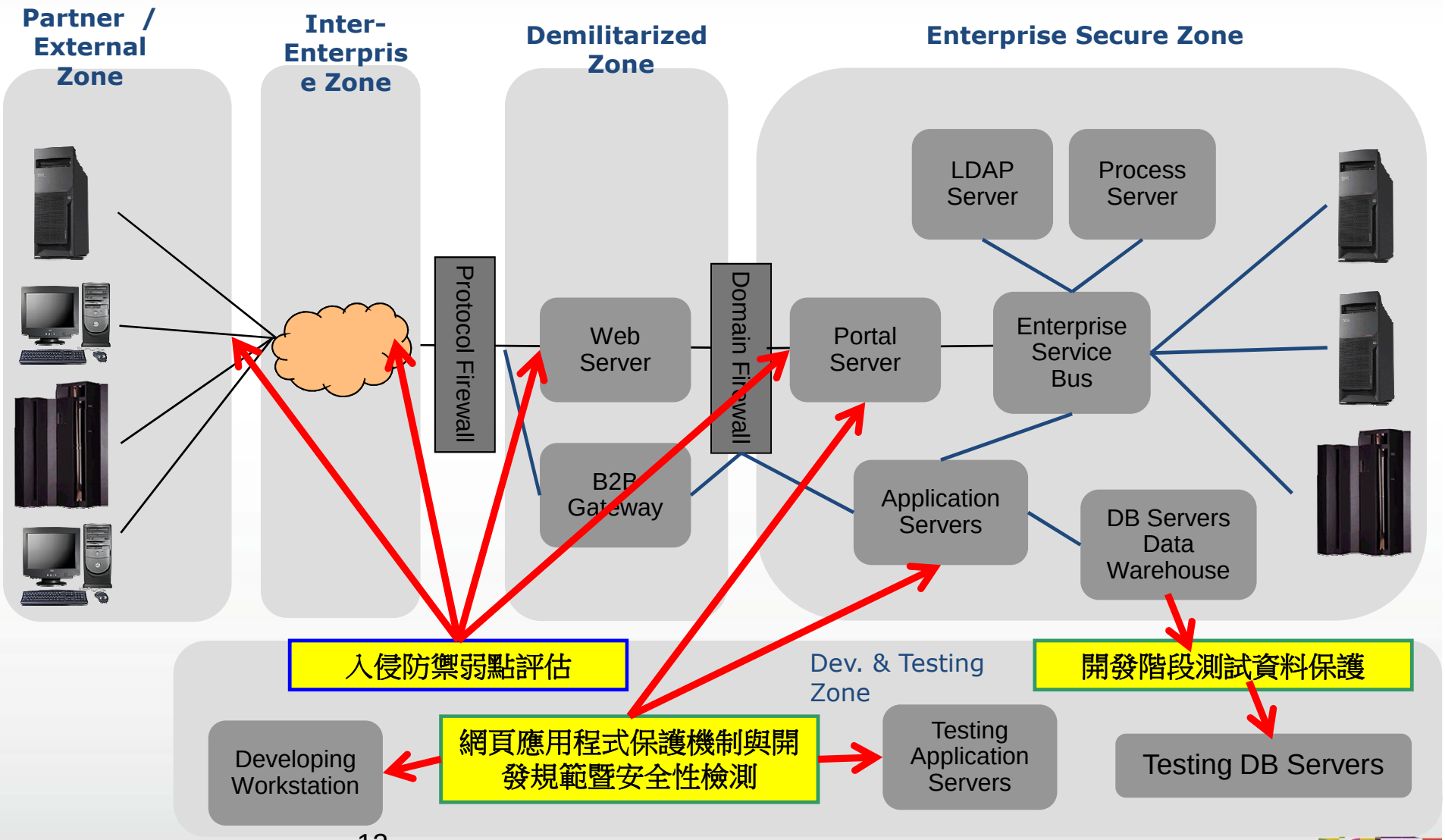


	Security Intelligence: Information and event management Advanced correlation and deep analytics External threat research			
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus
	People	**Data**	**Applications**	**Infrastructure**

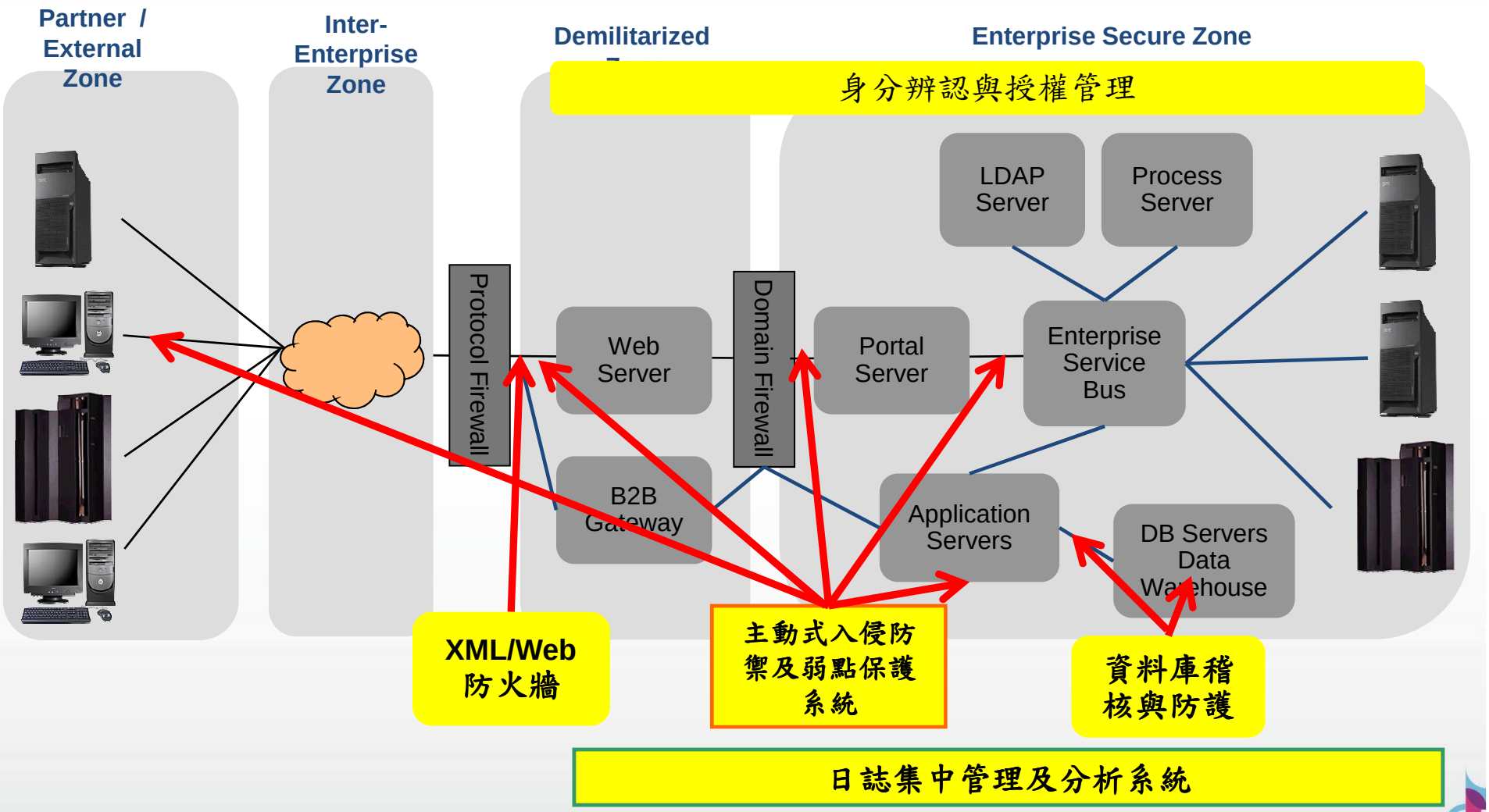
針對各面向所需的功能, IBM也提 出對應的解決方案



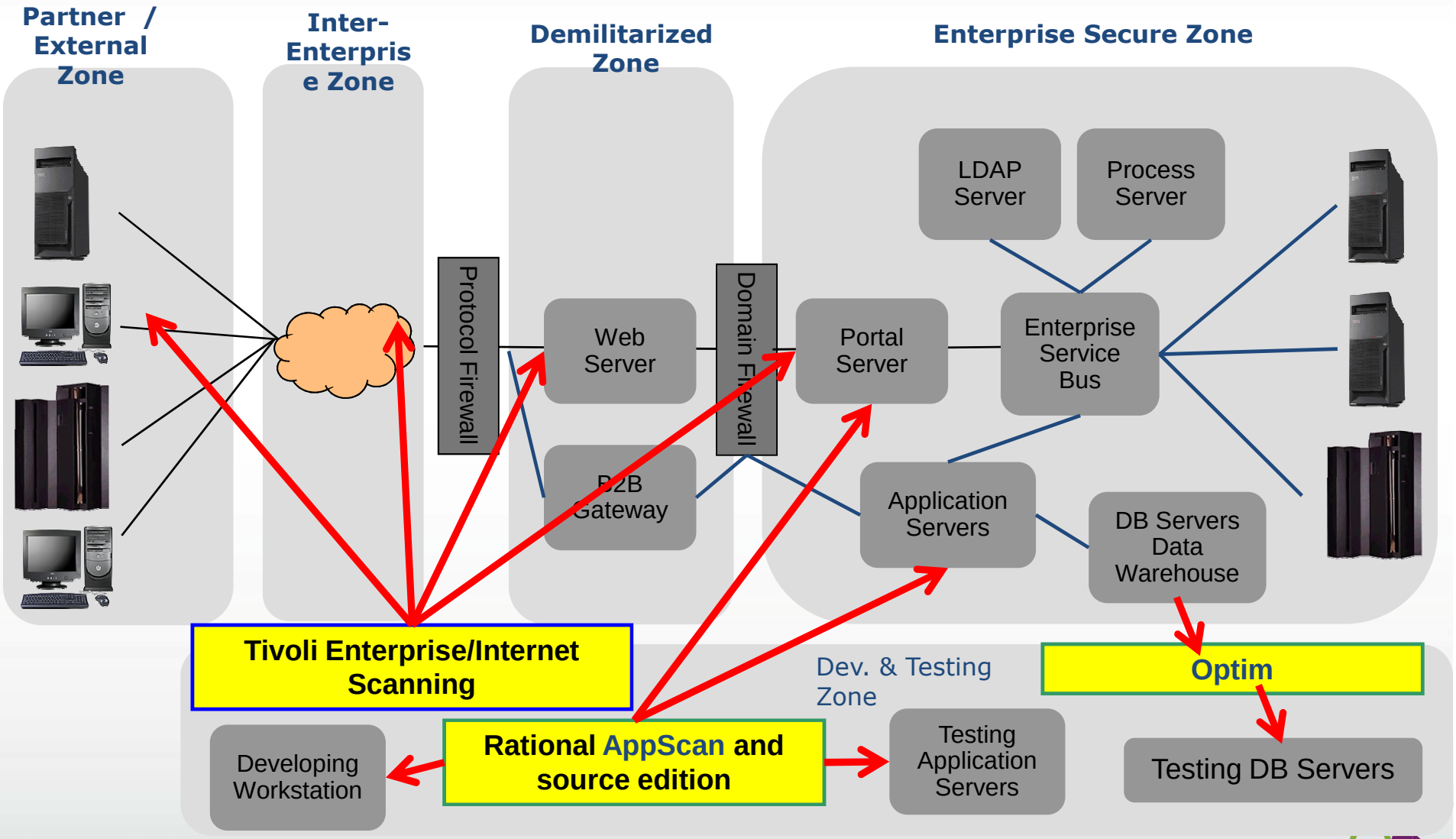
IBM資料安全解決方案實體架構圖–弱點評估與開發測試階段



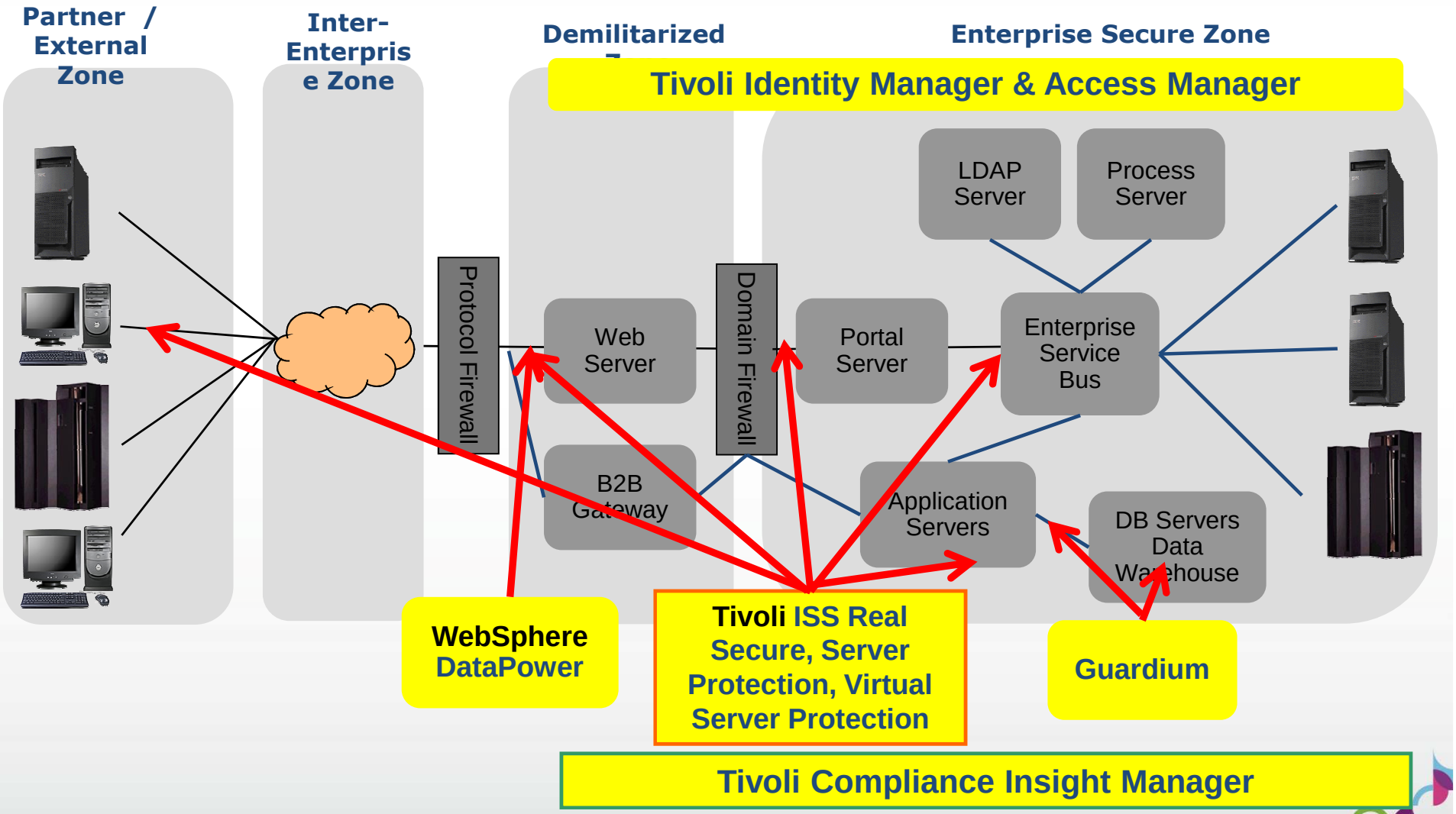
IBM資料安全解決方案實體架構圖 - 運行與維護階段



IBM資料安全解決方案實體架構圖–弱點評估與開發測試階段 -軟體產品對應



IBM資料安全解決方案實體架構圖 - 運行與維護階段 - 軟體產品對應



大綱

- 現階段面臨的資安挑戰
- IBM資安架構
- 資料庫稽核解決方案
- 網路入侵防護解決方案

資安/資訊主管對資料庫安全控管之期許

- 是否有存在獨立性、安全性及不可否認性
- 提出之報表是否有說服性
- 是否能對敏感性資料加以保護
- 所提供之解決方案是否能做到完全的資料隱密
- 是否會有資料遺漏的狀況
- 是否能對高權限使用者進行完全監控
- 是否會影響到正式環境作業

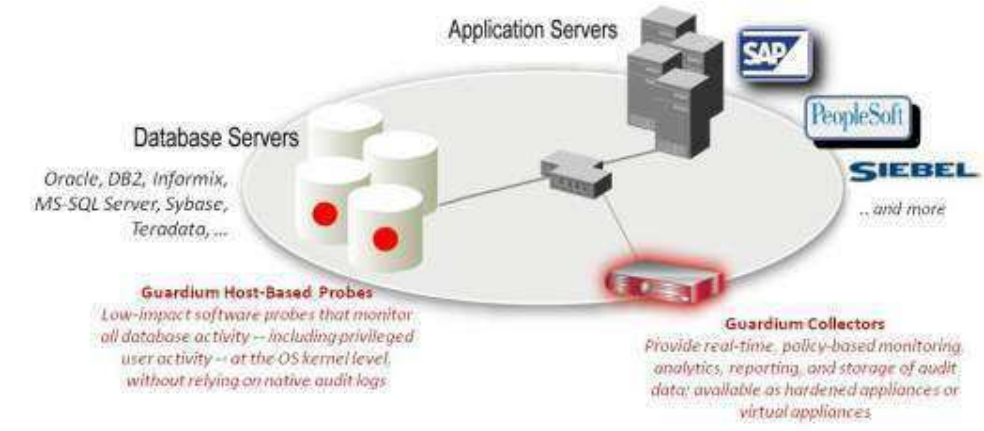
完整的資料庫安全生命週期

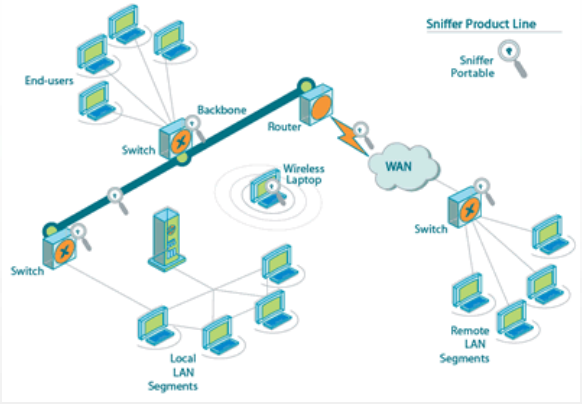
資料庫安全控管解決方案類型

- DB Audit Trial (資料庫原生記錄)
- Sniffer (擷取、分析網路封包)
- Agent (資料庫本機端側錄程式)

```
select object_name, object_type, status
from dba_objects
where object_name like 'FND_PROFILE_OPTION_VALUE_A%';
```

	OBJECT_NAME	OBJECT_TYPE	STATUS
1	FND_PROFILE_OPTION_VALUE_A	TABLE	VALID
2	FND_PROFILE_OPTION_VALUE_A	SYNONYM	VALID
3	FND_PROFILE_OPTION_VALUE_AC	TRIGGER	VALID
4	FND_PROFILE_OPTION_VALUE_AC1	VIEW	VALID
5	FND_PROFILE_OPTION_VALUE_AD	TRIGGER	VALID
6	FND_PROFILE_OPTION_VALUE_ADP	PROCEDURE	VALID
7	FND_PROFILE_OPTION_VALUE_AH	TRIGGER	VALID
8	FND_PROFILE_OPTION_VALUE_AI	TRIGGER	VALID
9	FND_PROFILE_OPTION_VALUE_AIP	PROCEDURE	VALID
10	FND_PROFILE_OPTION_VALUE_AT	TRIGGER	VALID
11	FND_PROFILE_OPTION_VALUE_AU	TRIGGER	VALID
12	FND_PROFILE_OPTION_VALUE_AUP	PROCEDURE	VALID
13	FND_PROFILE_OPTION_VALUE_AV1	VIEW	VALID



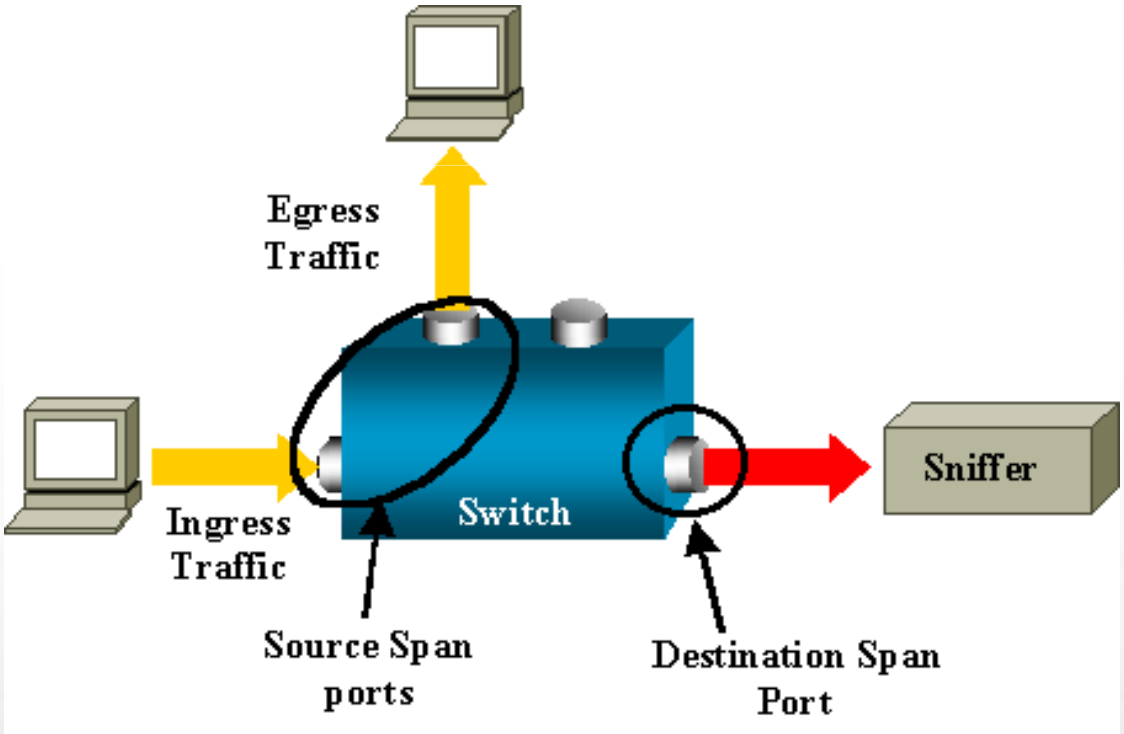


為何資料庫原生記錄(Audit Trial)不適用

- 影響資料庫效能
  - Which table, from which IP, using which command, which program, …
- 非獨立作業 – 可以很容易被DBA關閉
- 跨資料庫平台會有不一致的稽核策略 (增加複雜度)
- 無法提供主動式的即時安全警示 (review logs every 3 months?)
- 在連接池(connection pooling)的環境無法確認應用程式端的使用者 (PeopleSoft, SAP, Oracle Financials, etc.) – potential fraud
- 須具有大量稽核資料儲存需求
- 在篩選稽核資料時，須撰寫程式
- 在產生符規的稽核報表時，須撰寫程式

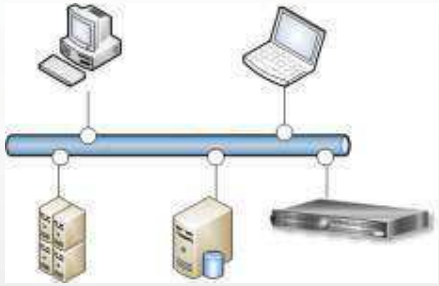
何謂Sniffer

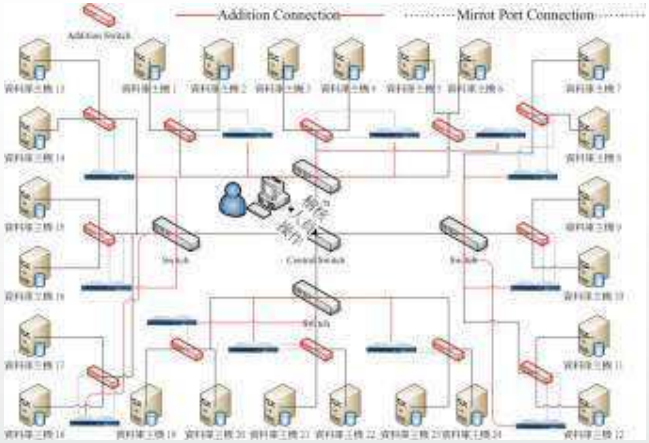
- 在Switch上使用SPAN port將網路封包進行複製
- SPAN port可針對所指定之一個或多個(switch需支援)port進行複製



使用Sniffer必需考慮下列事項

- 必須要確定現行使用之Switch有支援SPAN port
- 可能會因為額外SPAN port使用與現行之SPAN port用法相衝
- 可能因為額外SPAN port的需求而需另外購置Switch等相關
- 會改變現行網路架構並複雜化





使用Sniffer還會導致下列問題

- 收集完整性
  - 本機端資料無法收集
  - 加密過之資料無法收集
  - 網路雜訊太多會影響，網路封包掉失問題
- 安全性
  - 無加密處理
  - 接上SPAN Port可取得機敏資料,造成資安漏洞
- 網路影響
  - SPAN Port 會造成Switch設備Loading加重
- 導入衝擊
  - 對既有資訊架構影響較大,尤其是網路架構

使用Agent (in DB Server)的方式

<架構優勢>

安裝不須任何資料庫權限

不影響網路架構及交換器效能

記錄網路及本機登入活動

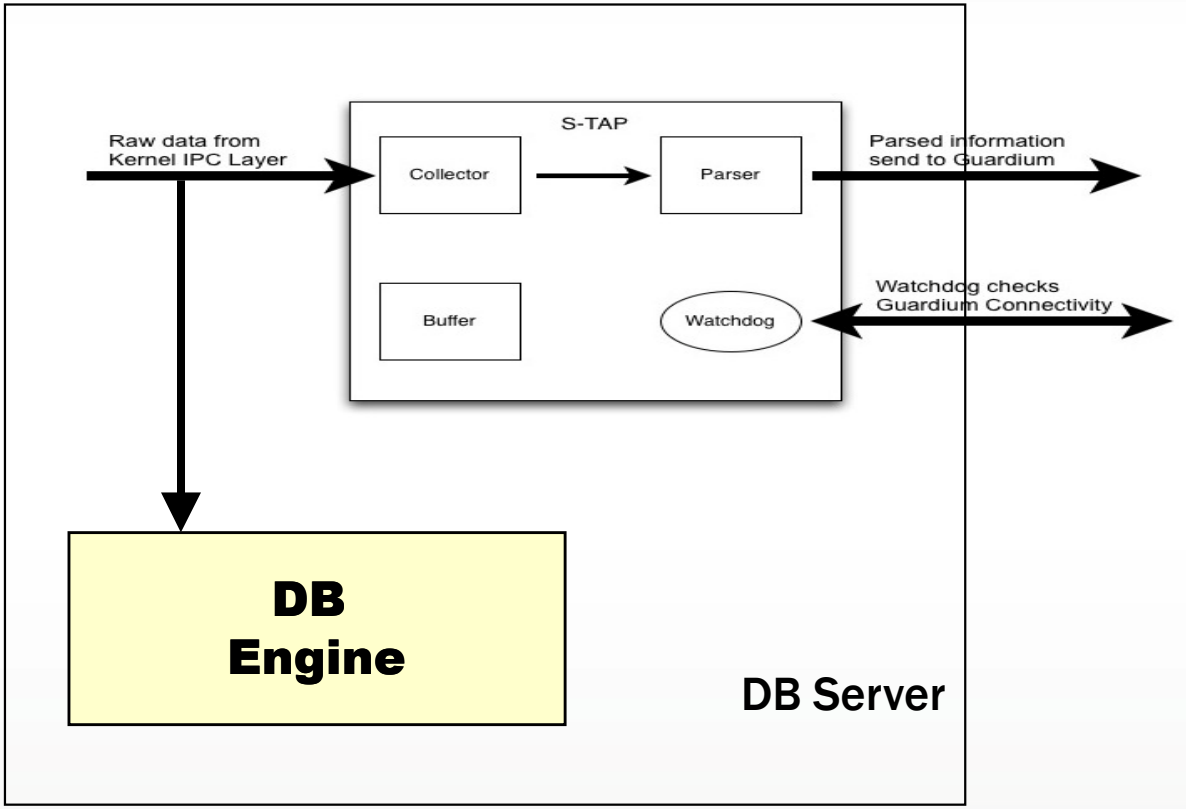
對CPU影響不高

Buffer 使用硬碟空間

Agent Fail 不影響主機運作 (Kernel 層次)

解析SQL 2005/2008及Oracle ASO加密機制(Encrypted Connections)

解析SU for UNIX



<注意事項>

有些產品雖然使用Agent的方式，但仍需要配合Sniffer (SPAN Port)，才能記錄所有網路與本機上的活動。

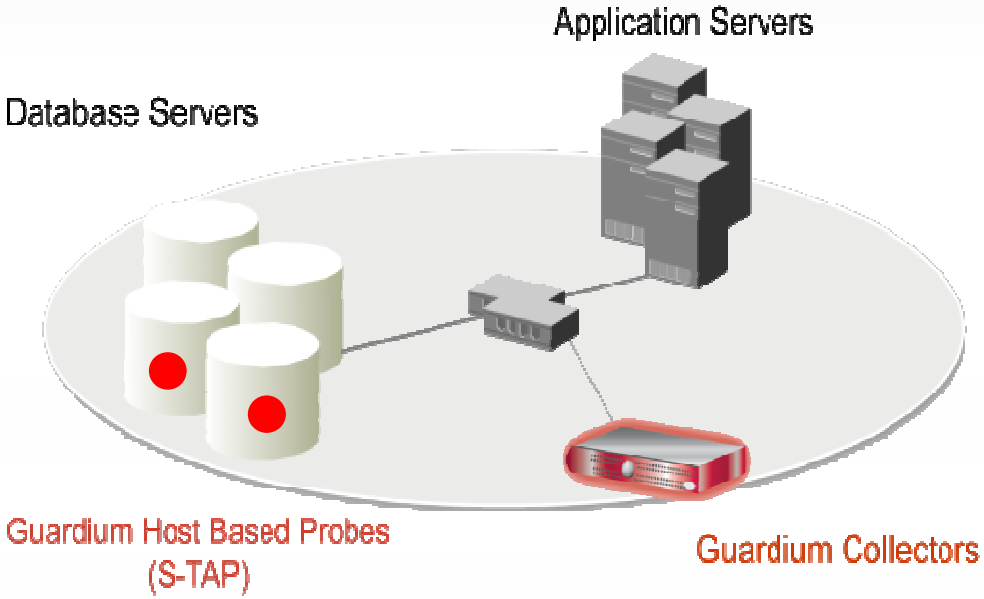
有些產品使用的Agent，是自Share Memory以Snapshot的方式取得資料，此種做法常有資料遺漏的現象。

產品是否得到國際公正單位的認證？相關的評比如何？

使用Agent及成套裝置(Appliance)

- 即時安全警示與阻絕
  - 主動防護企業資訊
- 安全的稽核資料庫 (獨立作業)
- 本機監控,使用Agent進行收集至100%資料,不需搭配使用SPAN port
- 詳盡的網路層級資訊
  - Client IP, OS login ID, source application, etc.
- 最小效能影響
- 不須變更資料庫或應用程式設定
- 具跨平台和企業層級的解決方案
  - 具稽核資料的彙總與正規化
  - 集中式的策略定義與執行能力

Guardium 解決方案– 您的不二選擇
Real-Time Database Monitoring



ORACLE
IBM DB2
SQL Server
TERADATA
SYBASE
MySQL
Informix

- 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
- 非侵入性
- DBMS獨立性
- 最小的系統影響(3 - 5%)
- 無需透過資料庫日誌和審計

Guardium提供深入的洞見 . . .

- 誰正在對資料庫進行疑似異常的更動?
- 某些未經過授權的資料變更是在何時進行的?
- DBA或外包廠商對資料庫做了什麼更動?
- 已經發生了多少錯誤的登入紀錄?
- 誰正在擷取信用卡資料?
- 哪些資料正在被哪個網路節點存取?
- 哪些資料正在被哪個應用程式存取?
- 正在進行的資料存取使以什麼方式在進行的?
- 比對資料存取的時間, 是否有哪些可疑的模式?
- 資料庫正在產生什麼錯誤訊息?
- 誰在何時對資料庫進行疑似資料隱碼攻擊?

Guardium 提供包含下列解決方案

- **Real-time database activity monitoring (DAM)**
  - 資料庫即時監控(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**
  - 稽核與制度方案：使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(美國沙賓法案 Sarbanes-Oxley)，PCI-DSS (支付卡產業之資料安全標準 Payment Card Industry Data Security Standard)。
- **Change control solutions**
  - 變更控制：在資料庫結構上、資料數值、特定者使用權、及系統設定上預防未經授權的變更。
- **Vulnerability management solutions**
  - 弱點安全管理方案：在弱點安全控管上的判讀及解決方案。
- **Database leak prevention**
  - 資料庫外洩防護系統：能指出在敏感的資料及對資料庫可能造成威脅的安全缺口，並加以防護。

大綱

- 現階段面臨的資安挑戰
- IBM資安架構
- 資料庫稽核解決方案
- 網路入侵防護解決方案

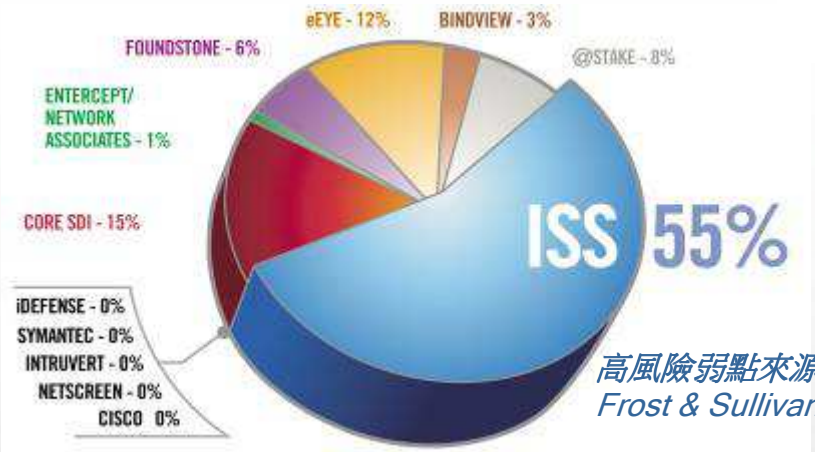
IBM擁有全球最大的資訊安全研發組織X-Force

- 專注於收集和分析資訊安全風險
- 每年發佈30 次以上的資訊安全建議和警告
- 每月找出200 多種新的攻擊手法
- 維護超過 30,000 個弱點的資安資料庫
- 開發了 6000 多個檢查項目用於檢測和發現攻擊手法
- 發佈每一季網路風險總結報告 (IRIS)
- 2009年，全球新增6,061個安全漏洞
- CVE創始人之一，CVE的審核者及工具提供者之一

世界頂尖的資訊安全研究機構

全球性的資訊安全營運中心

端點到端點的前瞻式資訊安全防禦產品



高風險弱點來源:
Frost & Sullivan 2006, Internet

X FORCE

IBM Global Security Reach

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

IBM入侵防護解決方案是基於X-Force實驗室的專利資產而建置

Research → **Technology** → **Solutions**

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

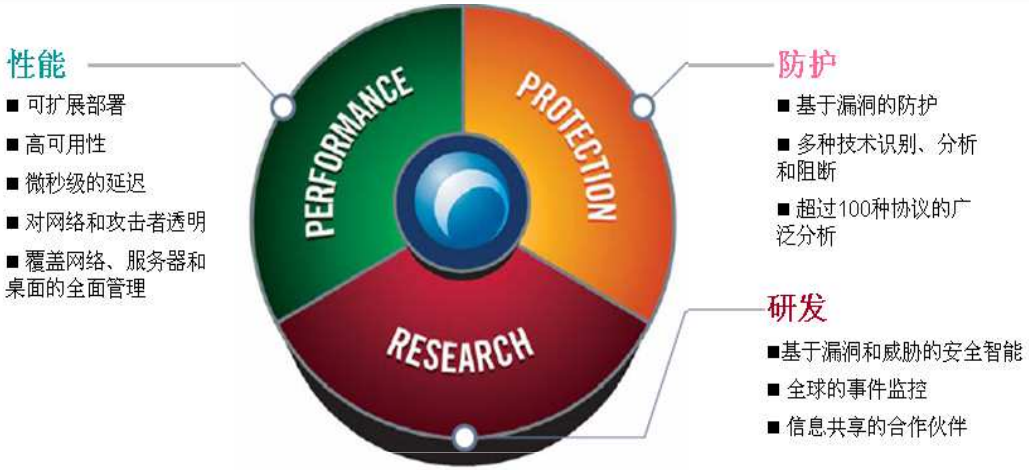
- Security Content Update Development
- Security Content Update QA

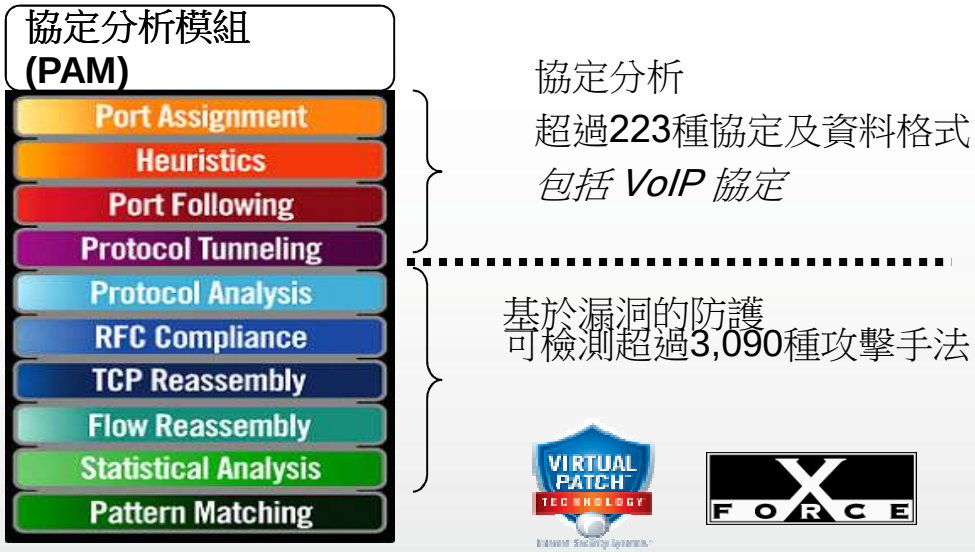
X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

The X-Force team delivers reduced operational complexity – helping to build integrated technologies that feature "baked-in" simplification

IBM Security NIPS (入侵防禦系統)





IBM IPS主要特點

■應用ISS X-Force研發結果，基於弱點的防護，執行“前瞻式防護”

■ Virtual Patch-虛擬修補程式技術保證“零天防禦”

■核心技術為-“*Hybrid Protocol Analysis Module*”

■ISS了解資料流和資料流量的狀態

■ISS能夠提供最精確的防禦
– 可支援223種協定和資料格式，可檢測/防禦超過3090種攻擊手法

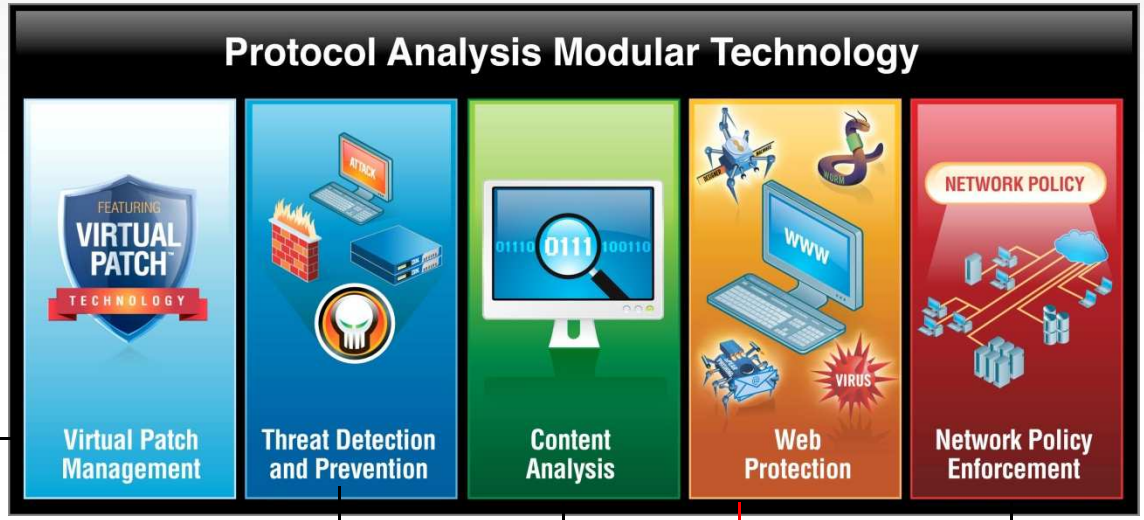
■超強性能- GX7800為業界最大throughout設備 - >20Gbps (Inspected)

■全球市場佔有率連年第一

IBM X-Force

Extensible Protection Platform

PAM is the engine behind the preemptive protection afforded by many of the solutions of the IBM Proventia product family. PAM is comprised of 5 key technologies.



Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2008, **53%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Content Analysis

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy

Web Application Security

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Network Policy Enforcement

What It Does:
Manages security policy and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

Intrusion Prevention Solutions that Fit your Needs

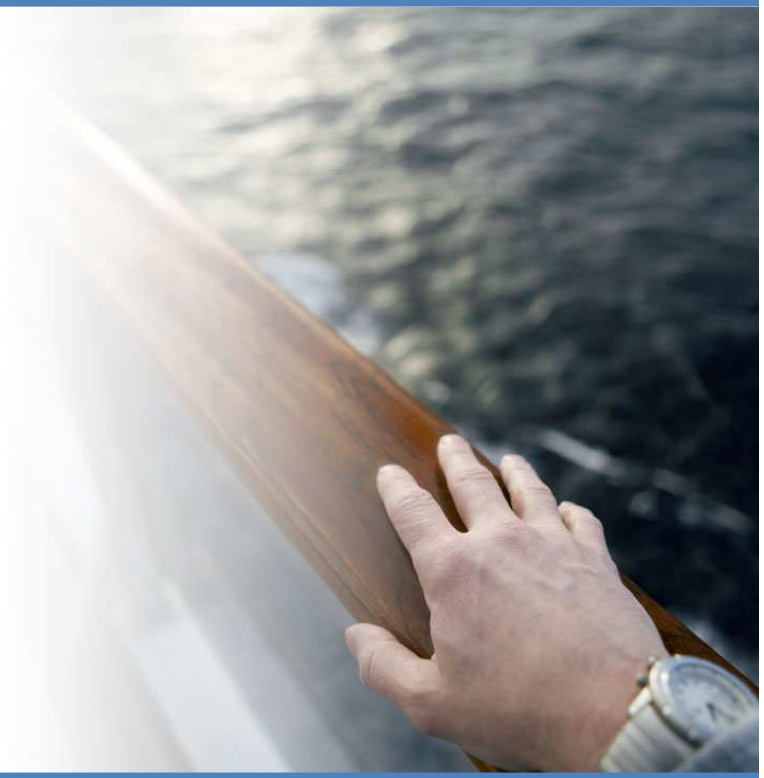
- Block threats before they impact your organization
- Uncompromising security backed by X-Force®
- Inspected throughput from 200 Mbps to 20Gbps+
- Protection for up to 8 network segments
- Scale from remote offices to the network core

GX7800 and GX7412

IBM Security Network IPS Models									
	Remote	Perimeter			Core				
Model	**GX4004-200**	**GX4004**	**GX5008**	**GX5108**	**GX5208**	**GX7412-5** NEW	**GX7412-10** NEW	**GX7412** NEW	**GX7800** NEW
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

Thank You!

Q&A



IBM Security Solutions

Ahead of the threat.™