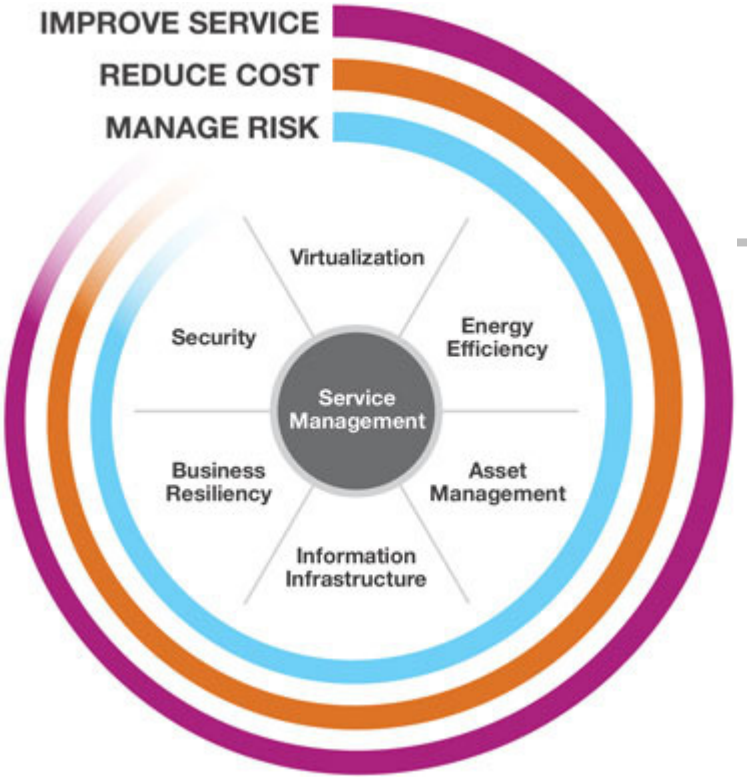
資料運用與保護策略分析

捍衛智慧財產，保障商譽與隱私



A Smarter Planet

SmarterSecurity&Resilience

"Of course I'm wearing rubber gloves, haven't you heard about the computer virus?"

IBM

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：

- 資料保護及應用程式運用護整體防禦架構
- 資料安全與洩漏保護策略
- 應用程式運用與網路安全的防護

每當新科技問世，機會與風險之間的界線便會些許挪移。在我們積極探索新技術所蘊含的機會與潛能的同時，有心人士也急於鎖定弱點發動攻擊。因此，隨著科技推陳出新，組織因應安全威脅的策略也可能產生根本的改變。

新興科技的推陳出新

MILS VPN Laptop Encryption SOX Physical Access IPSEC DAC HIPPA SSL SAML Identity Management Password Smart Card PCIDSS MLS SaaS Token FIPS 140-2 Biometrics Trusted Computing XML Gateways PKI Cross Domain Systems Kerberos Thin Clients Accreditation H/W Crypto Digital Certificate Trusted OS LSPP/EAL4+ MAC Guards Hardening SABI/TSABI Wireless Secure Blades Tripwire Secure Collaboration Cyber Security Federation TCP Wrapper Cloud RSBAC FISMA Compliance SOA Security

* Not a complete collection

科技驅勢所帶來企業運作的安全挑戰


即時感應實體資產安全防護


捍衛行動裝置及個人資訊設備


保障網絡安全


應用程式運用安全可預測性


資訊安全及隱私

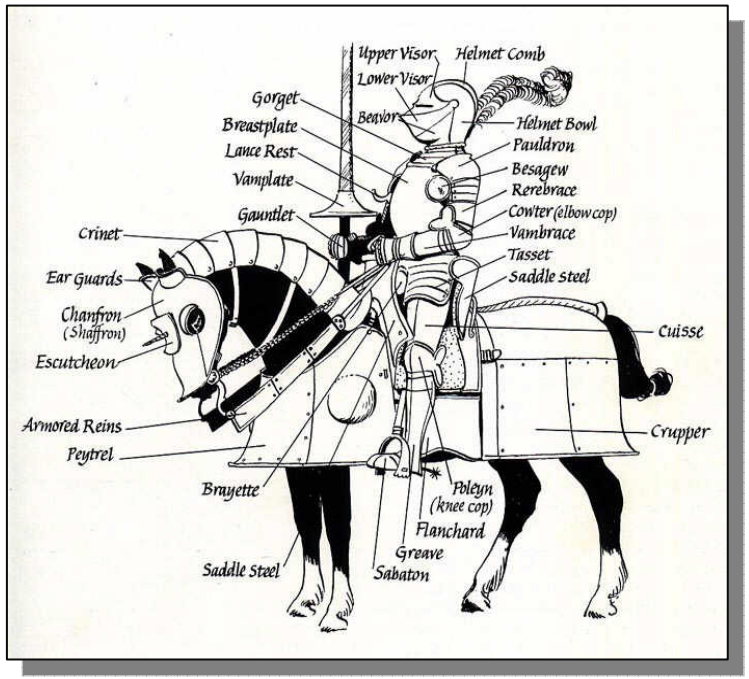

管理風險及法規需求

A Smarter Planet

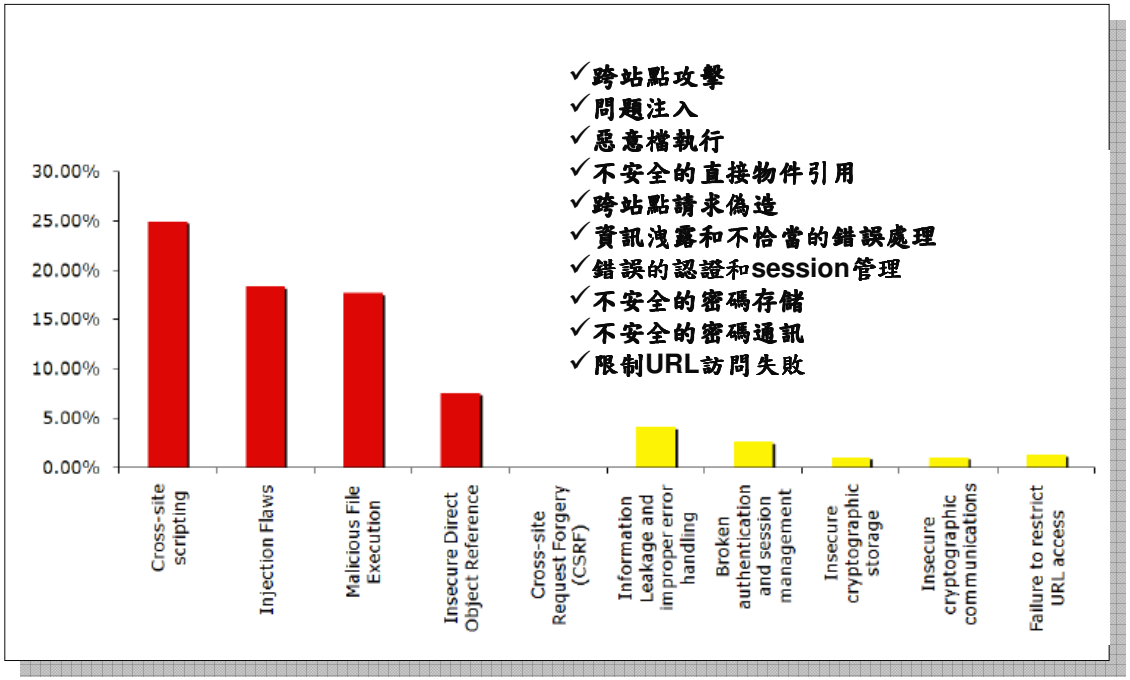
SmarterSecurity&Resilience

打造完整資訊防禦架構與管理，須從「單點且缺乏業務/系統處理流程整合」的產品導入方式，改為全方位資料處理的流程控管。 從**被動式的資安補強措施**及方案， 改為**主動式的資料處理流程整合**，防止有意或無心使用者的外洩行為。

單點且缺乏業務/系統處理流程整合資料保護解決方案



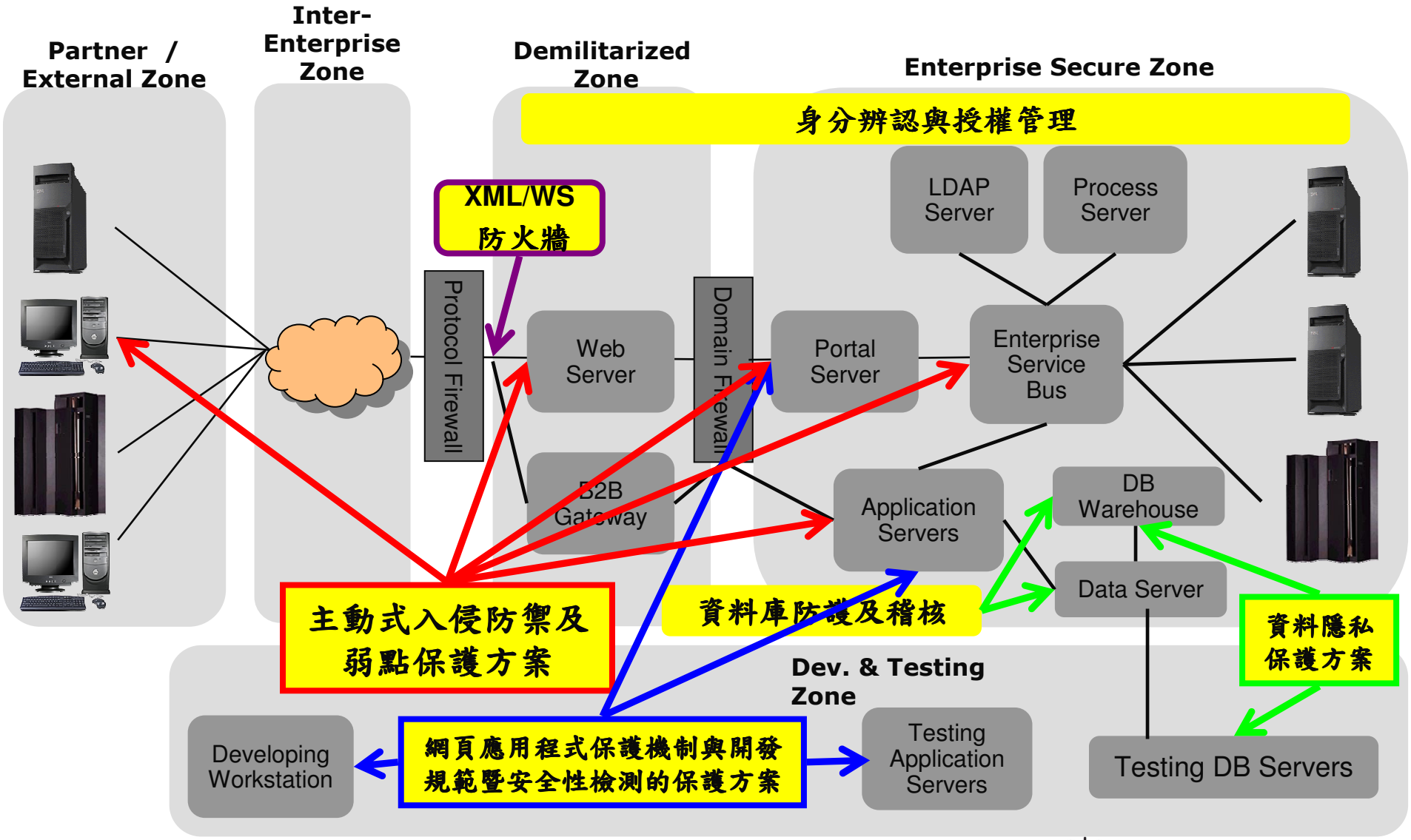
個資洩漏的相關統計資訊及研究報告十大應用安全隱憂



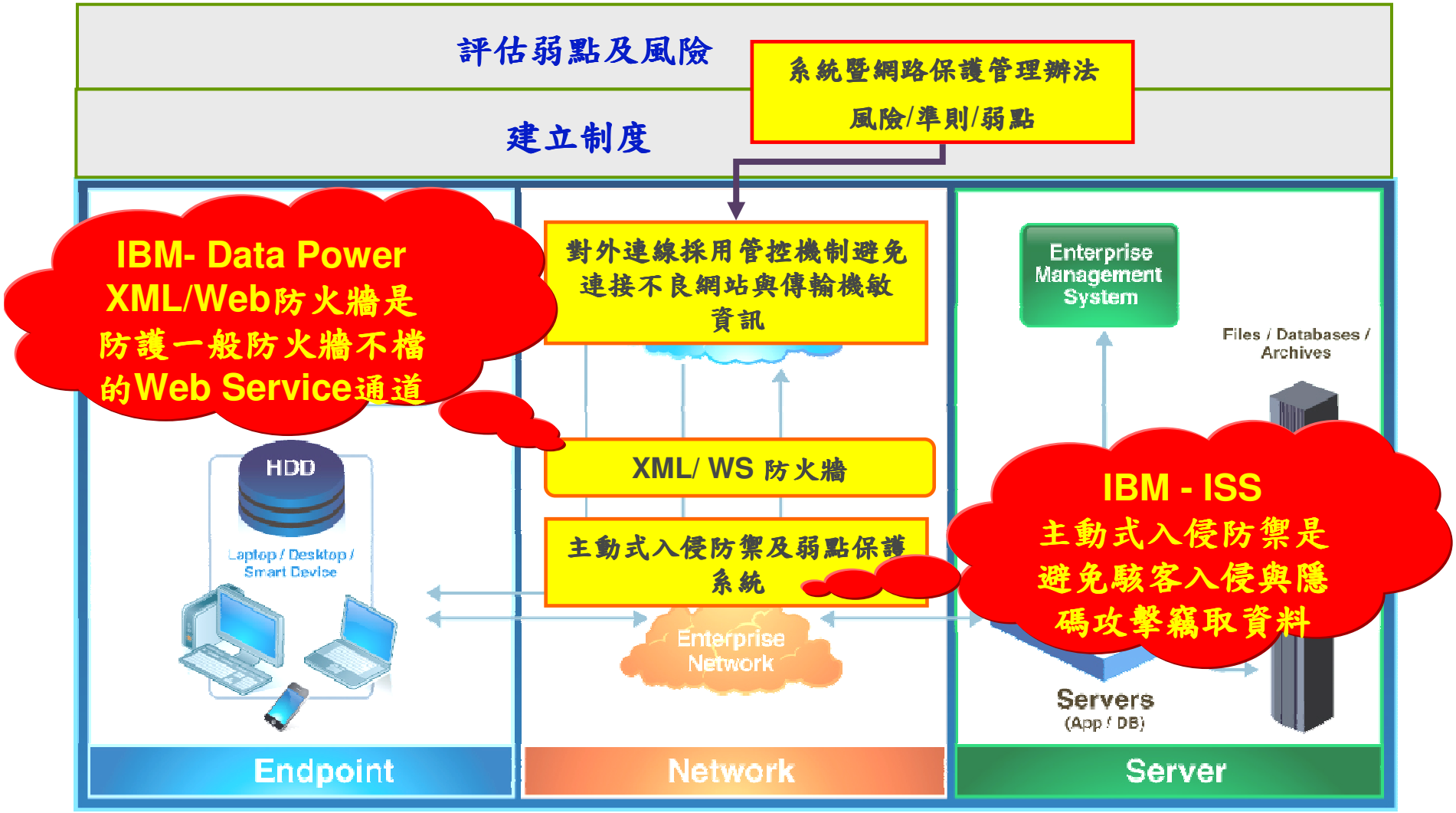
未有整體防禦架構

缺乏資料運用整體架構

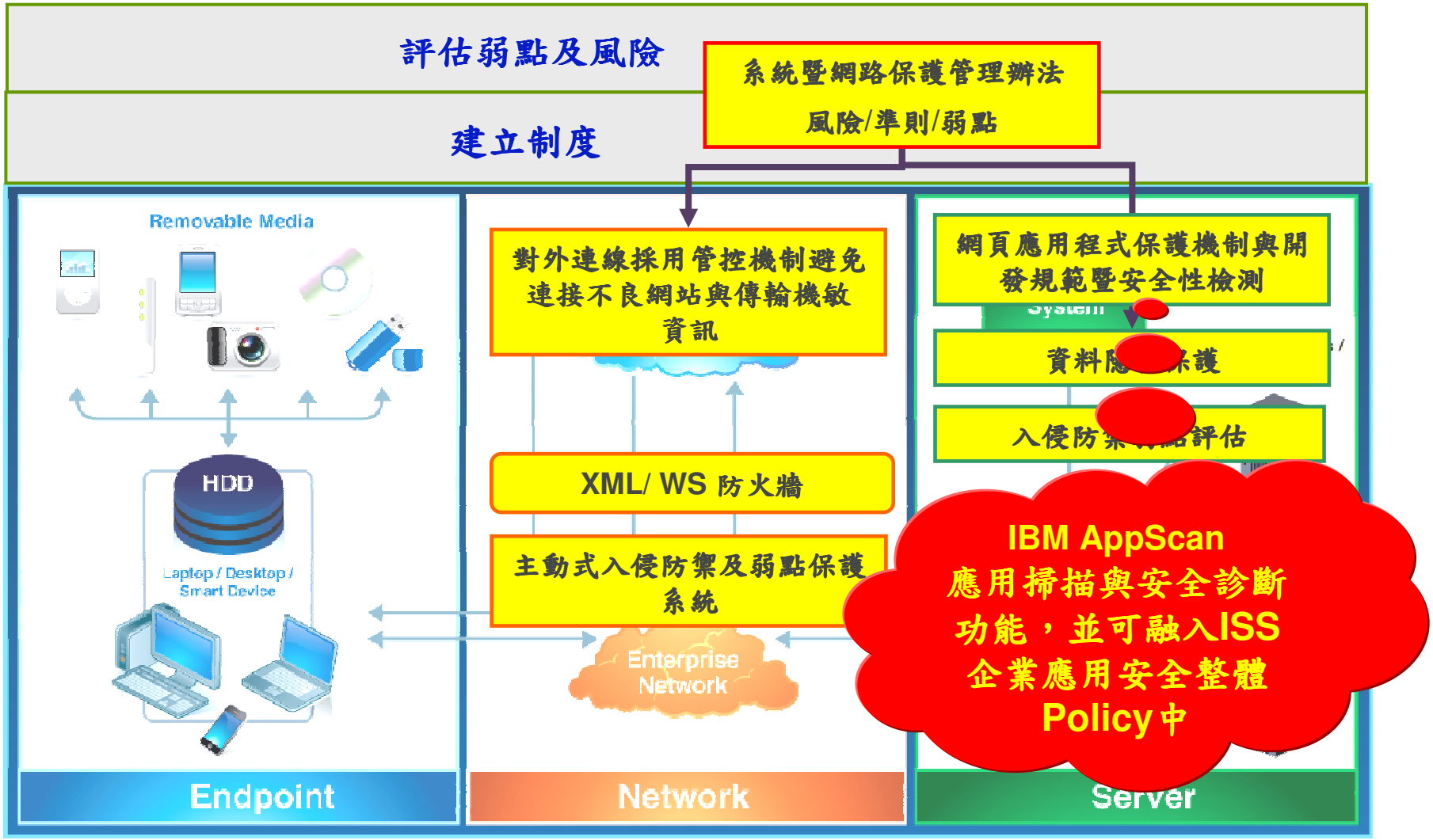
IBM『資料運用與保護解決方案』，主要針對所涉及資料之蒐集、處理及利用等資料運用流程，提出網路資料傳輸入侵防護及資料外洩保管及相關流程整合解決方案。



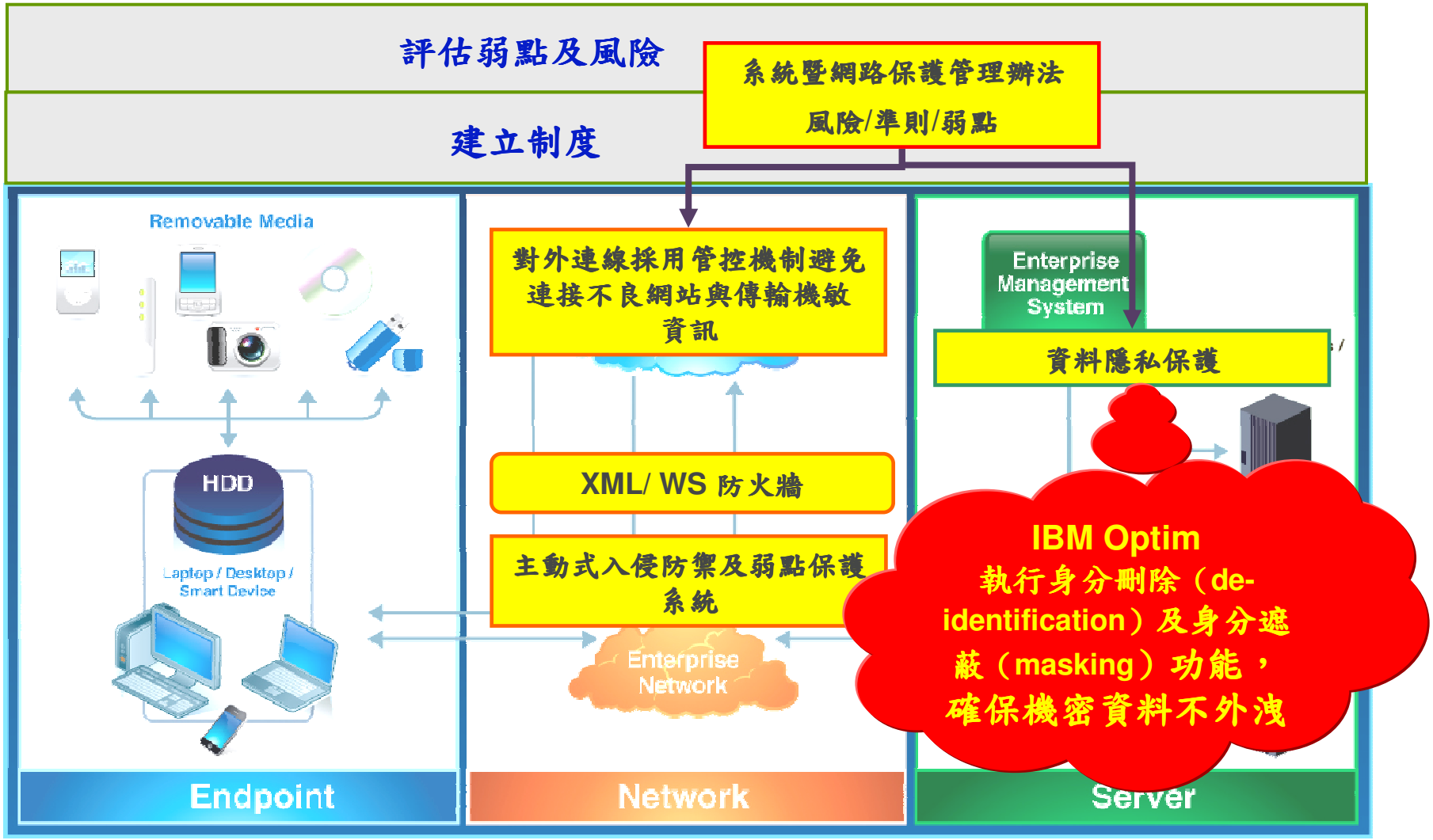
在開放式協同作業環境、Web 2.0混搭（mash-up）技術及智慧型資料串流技術的推波助瀾下，日益增加的各型資料持續且不受限制地在企業間網路內外流通，傳統的入侵預防系統（intrusion prevention systems-IPS）與防火牆技術已不足以因應這些新型態的攻擊。



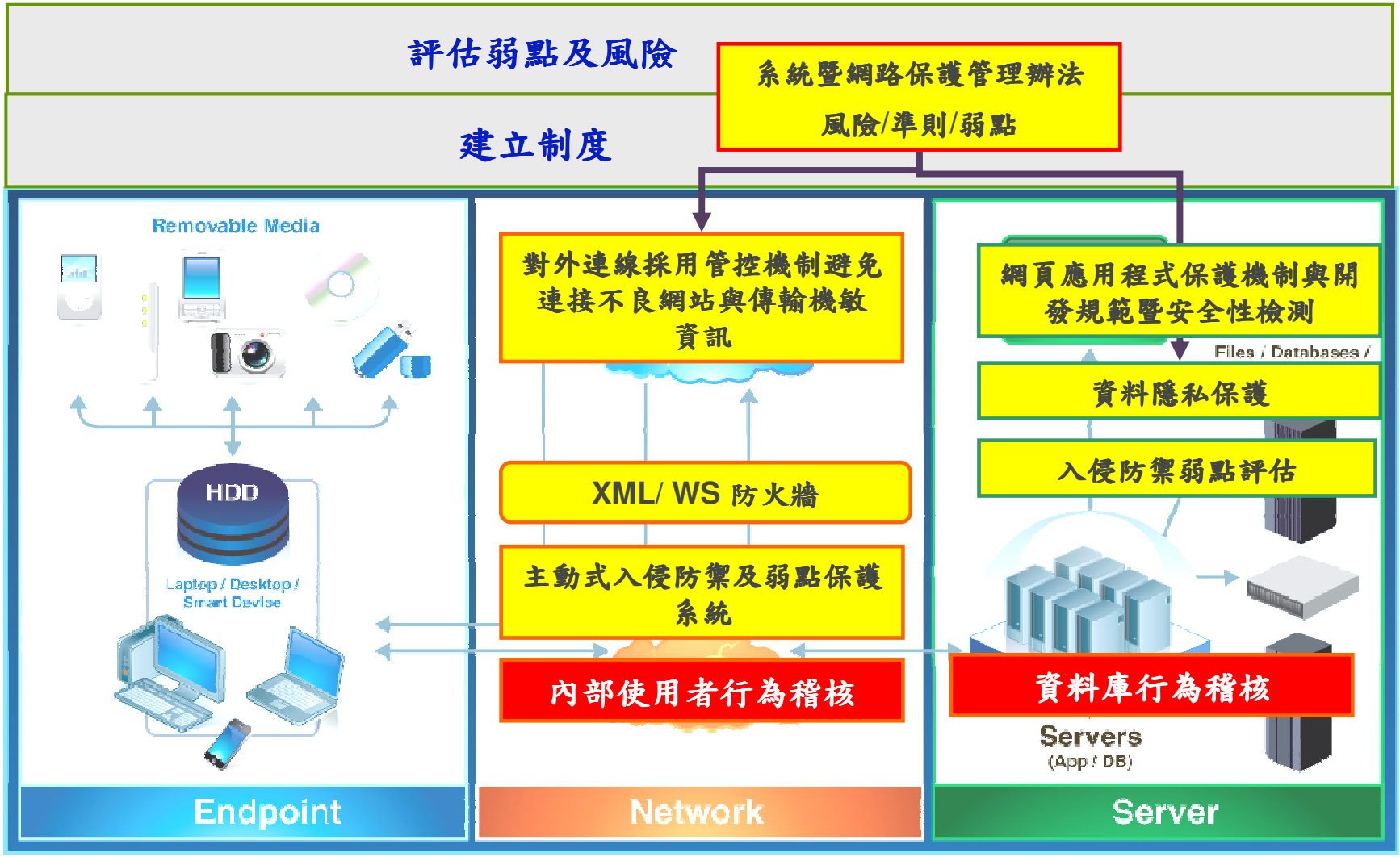
隨著應用程式開發模式從整體（monolithic）模式到組合（composite）模式的進展，雖提升程式設計的效率，卻容易造成程式的安全弱點。為因應這些挑戰，安全開發功能須被納入應用開發工具與平台中，才能在開發過程各個階段中執行安全診斷，全面防堵安全弱點



資料庫日益膨脹，資料持續且不受限制地在企業間網路內外流通資料外洩情事時有所聞，導致資料受損、不當揭露及智慧財產誤用的風險逐步升高。業界必須把焦點放在隱私權管理的遮蔽（mask）技術上，尤其是應用程式開發等資料保護工作中較鬆懈的非生產環境。



企業需以融合整合式網絡、伺服器與端點保護技術，並具備高度擴充及協同合作功能的安全平台為基礎，並結合資料庫行為稽核及使用者行為稽核將電腦操作畫面輸出入資料錄起來更能達到舉證、稽核的效果，擘畫完備的防護策略。



Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 資料保護及應用程式運用護整體防禦架構
- **資料安全與洩漏保護策略**
- 應用程式運用與網路安全的防護

檢視『修正版個資法』第二十條採取「Opt-Out」客戶選擇退出機制，客戶得自主決定是否揭露其個人資料。其基本的理念，源於隱私權(Data Privacy)

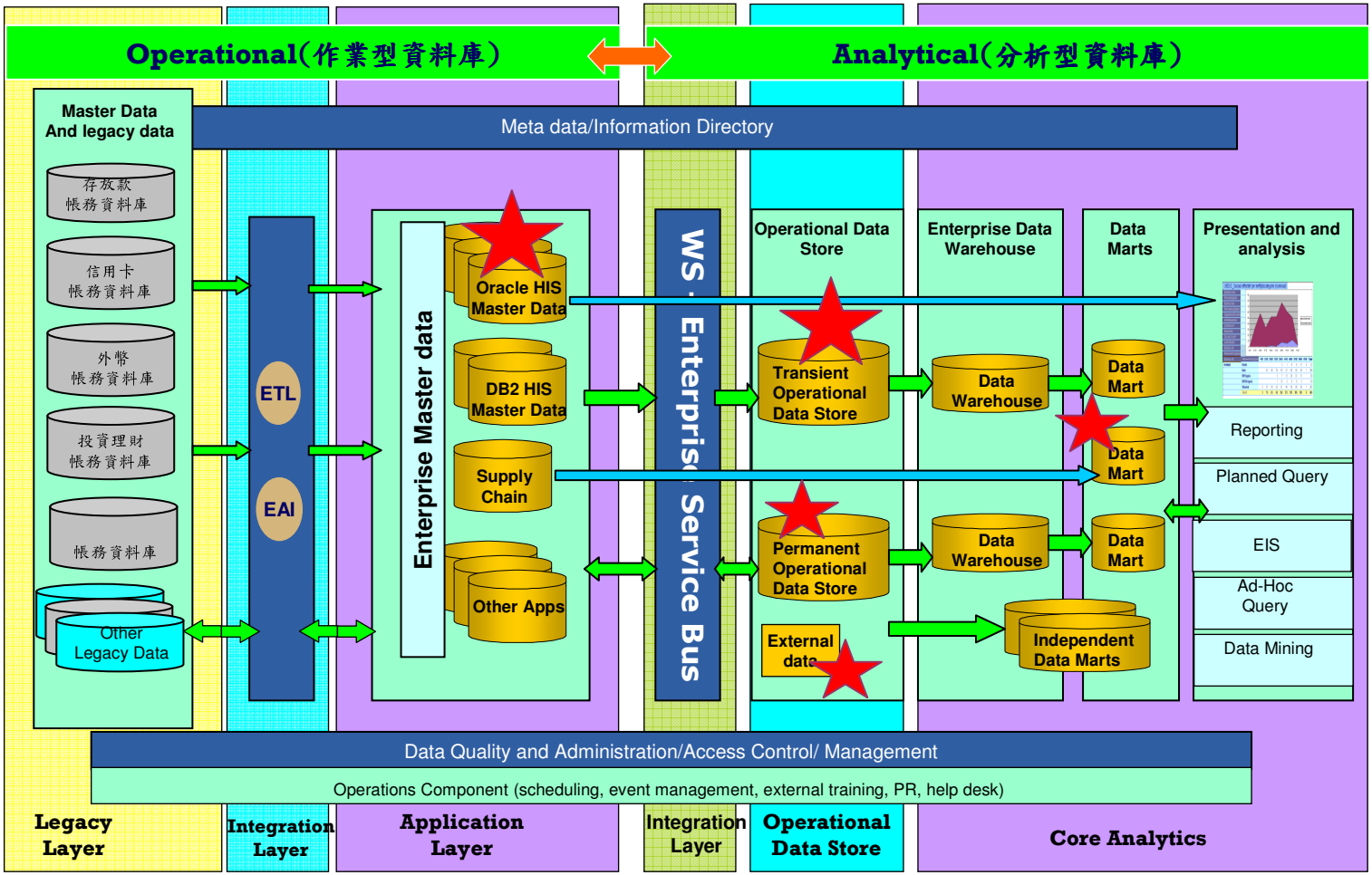
「金融控股公司法」客戶資料之分類及內容

- 基本資料
  - 姓名、出生年月日、國民身分證統一編號、電話及地址
- 帳務資料
  - 帳戶號碼或類似功能號碼、信用卡帳號、存款帳號、交易帳號號碼
  - 存借款及往來之交易資料
  - 財務情況
- 信用資料
  - 退票記錄、註銷記錄、拒絕往來記錄及業務經營狀況
- 投資資料
  - 投資或出售投資之標的、金額及時間等資料
- 保險資料
  - 保險種類、年期、保額、繳費方式、理賠狀況及拒保紀錄等相關資料

金管會已於98.01.21修正公布「金融控股公司法」第43條，採取客戶選擇退出（opt-out）機制，即客戶基本資料得交互運用，但客戶之往來交易資料及其他相關資料，則應**先經客戶書面同意**，**惟如客戶通知**不得繼續共同使用其基本資料、往來交易資料或其他相關資料時，應即停止共同使用。

當客戶客戶選擇退出機制「Opt-Out」時，散佈在各類不同「分析型」資料庫的隱私資料，依據客戶指示執行身份刪除(De-Identification), 去個人化(depersonalize), 匿名化(Anonymize)及身份遮蔽(Masking)並同時保持資料完整性，實為保護隱私權的關鍵！！

★ 隱私資料的控制點(Control Point)



檢視企業資料架構(Information Architecture)及資訊流(Data Flow)，分析隱私資料的分類與分佈，找出隱私資料的控制點(Control Point)

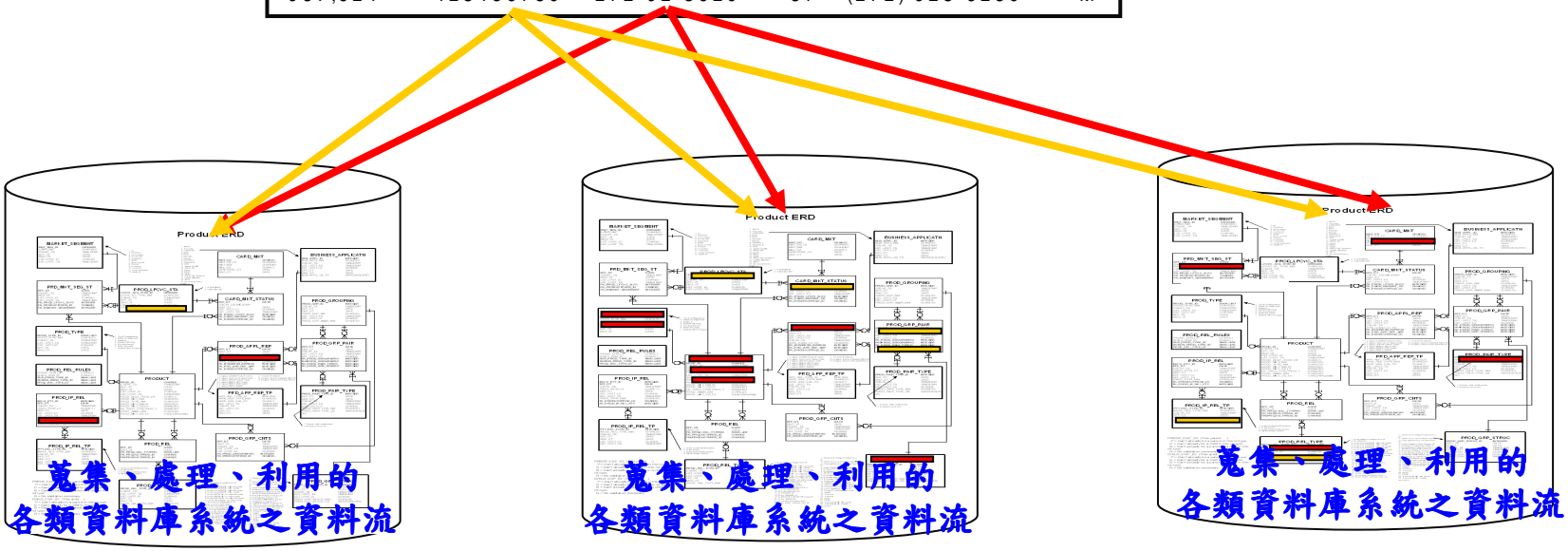
IBM Optim- Data Privacy對企業資料架構中隱私資料的控制點(Control Point) ，提供一個簡單、可擴展、易於整合的隱私資料保護解決方案；打造出可信賴的架構環境，讓企業能以充分反映資訊價值及保障用戶隱私的方式，安心地把資訊資產用於業務最佳化。

But, Finding Sensitive Data is Hard

Sensitive Data Repository

Row	Member	SS #	Age	Phone	Sex
1	595846226	123-45-6789	15	(123) 456-7890	M
2	567472596	138-27-1604	8	(138) 271-6037	F
3	540450091	154-86-4196	22	(154) 864-1961	M
4	514714372	173-44-7900	55	(173) 447-8996	F
5	490204164	194-26-1648	4	(194) 261-6476	F
6	466861109	217-57-3046	66	(217) 573-0453	M
987,623	444629628	243-68-1812	25	(243) 681-8107	F
987,624	423456789	272-92-3629	87	(272) 923-6280	M

業務及交易流程之隱私資料運用



結合企業之業務推廣、資訊交互運的業務及交易流程 ， 針對蒐集、處理、利用的各類資料庫系統之資料流進行隱私資料控管

隱私資料保護 - IBM Optim 提供了自動化的資料轉換、變形能力，能夠輕鬆地跨越多個資料庫將企業中涉及的各種個人資訊或保密資訊實施脫密、漂白處理。不但幫助企業實現法規遵，還能夠為測試或應用外包等提供無損企業利益的脫密資料版本，實現企業隱私資料的有效保護

Lookup 陳筱玲→陳雲林

Aging 加三天

Semantic 可驗證的假身份證字號

Hash Lookup 地址甲→Hash→地址乙

Random 亂數生成序號

隱私資料保護 - IBM Optim 針對不同資料格式提供不同遮蔽機制，能夠輕鬆地執行身份刪除(De-Identification), 去個人化(Depersonalize), 匿名化(Anonymize)及身份遮蔽(Masking)並同時保持資料完整性

Intelligent Data Masking

A comprehensive set of data masking techniques to transform or de-identify data:

- String literal values
- Character substrings
- Random or sequential numbers
- Arithmetic expressions
- Concatenated expressions
- Date aging
- Lookup values
- Intelligence

Example 1

Customer Information

Customer No.	123456	**PID**	E165851537
Name	李大雄		
Address	四維三路2號		
City	高雄市	**Zip**	80203

Data is masked with contextually correct data to preserve integrity of test data

Example 2

Personal Info Table

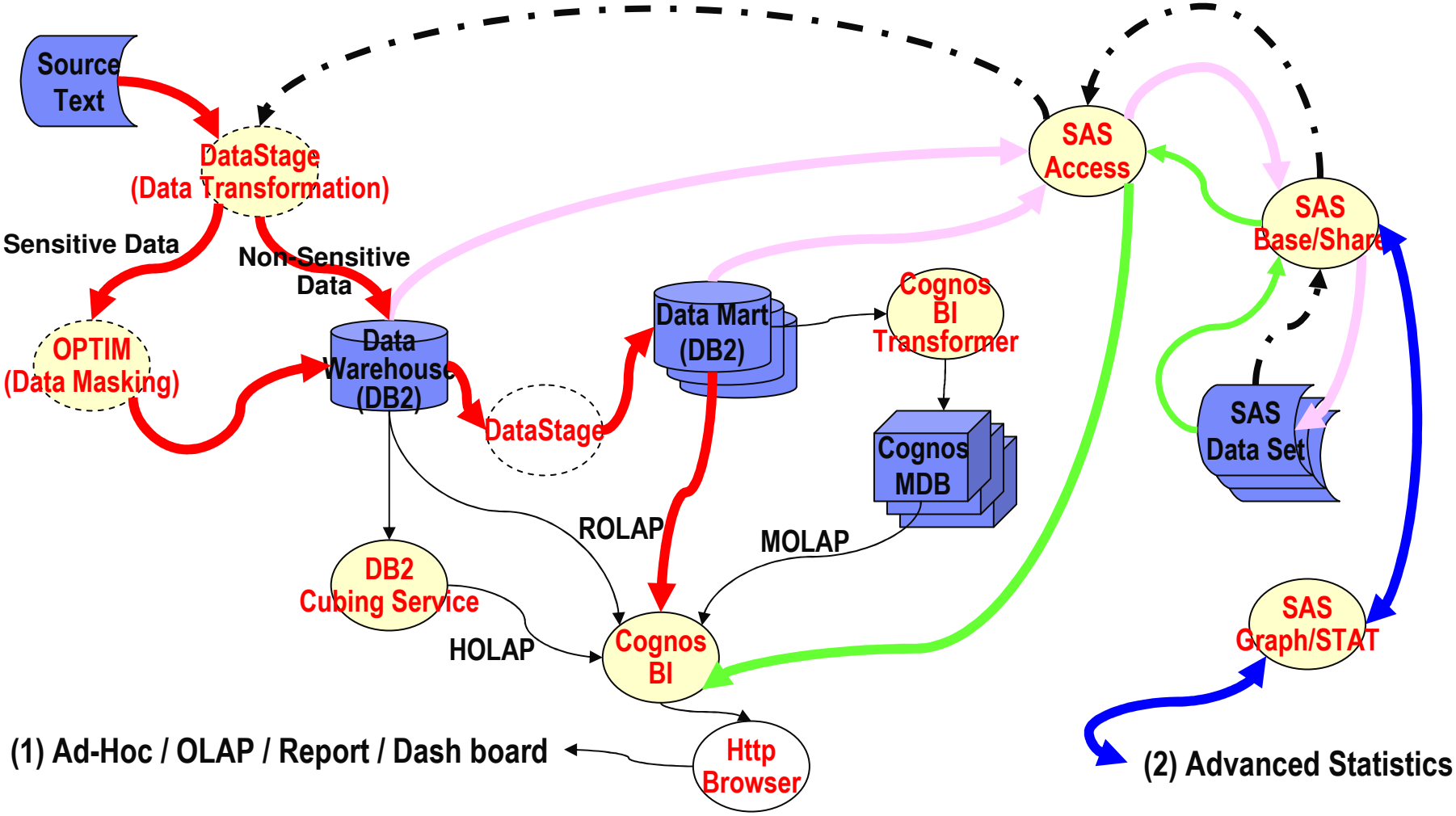
Account	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	**Pablo**	**Picasso**

Referential integrity is maintained with key propagation

Event Table

Account	FstNEvtOwn	LstNEvtOwn
10002	**Pablo**	**Picasso**
10002	**Pablo**	**Picasso**

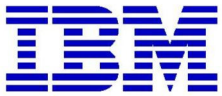
隱私資料保護 - IBM Optim 參考使用案例之架構



除了以上能力以外，IBM Optim還為大多數主流套裝應用—如:SAP，Siebel，Oracle ERP等提供了定制能力，同時能夠支援幾乎所有主流伺服器、作業系統與資料庫產品，並提供多平臺的集成訪問能力。—— 除了IBM Optim，目前還沒有任何其他產品能夠提供如此豐富的軟硬體平臺與套裝產品支援！

成功案例介紹

套裝軟體



- IBM 通過Optim 管理其Siebel系統中的歷史資料，有效控制了每年20%的資料增長，並提高了全球8500個用戶的應用系統回應時間 ，首次歸檔即實現了2390萬activities和1001萬Leads記錄的有效瘦身

資料管理平臺

- 金融風暴已迫使金融行業重新審視資料管理的重要性. 就美洲銀行為例, 現存的資料管理方式分散且不安全, 並會給企業帶來嚴重的訴訟成本. 經過半年多的考查和評估, 美洲銀行最終在2008年底選定OPTIM為其打造企業級資料管理平臺

聯邦海量資料處理

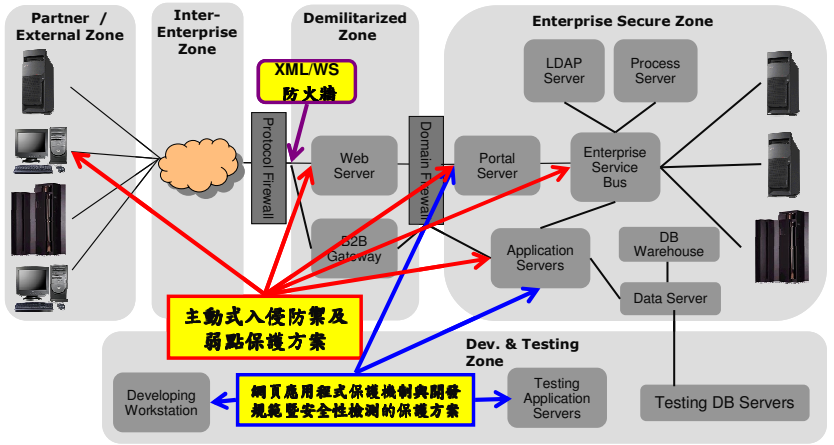
- 印度最大的移動通信公司, 每天有10億通話記錄要處理. 資料量雖大, 但更加重要的是要把經過漫遊的通話記錄構成一條計費記錄. 電話漫遊過程中, 通話可能經過不同廠商提供的基站, 所以一通電話可能由來自不同資料庫而且不同資料格式的資料, 經過處理過程形成. OPTIM為客戶的需求提供了最佳方案

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda

- 資料保護及應用程式運用護整體防禦架構
- 資料安全與洩漏保護策略
- **應用程式運用與網路安全的防護**

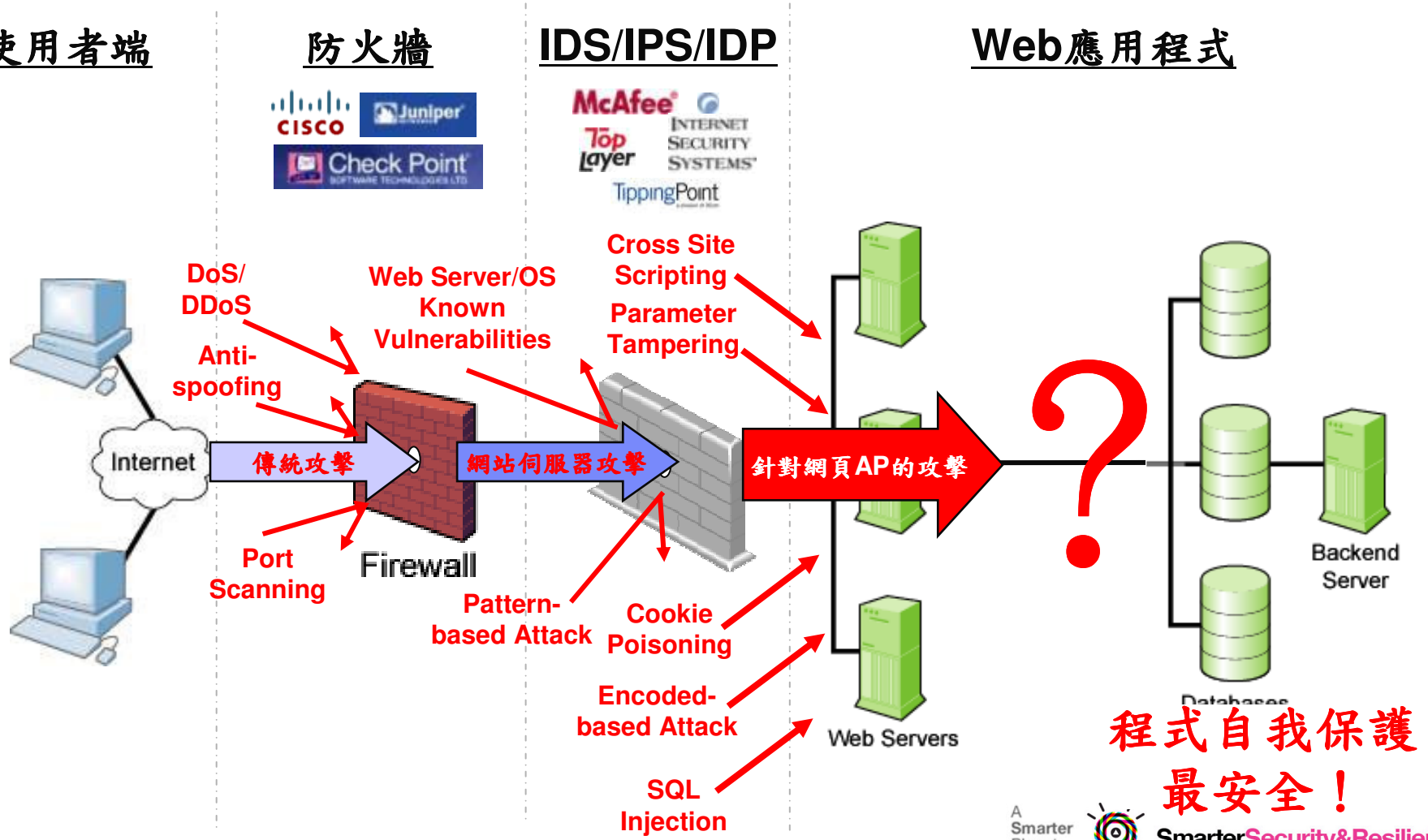


A Smarter Planet

SmarterSecurity&Resilience

2008年，一種名為SEO程式碼植入（injection）或毒害（poisoning）的新型態資安威脅，影響全球高達120萬個網站，其中不乏一些相當知名者。隨著災情逐漸緩和，全世界開始慢慢體會到應用程式已成為駭客攻擊的首要目標。

從Web應用程式運作架構，看各類攻擊對網路節點的防禦能力



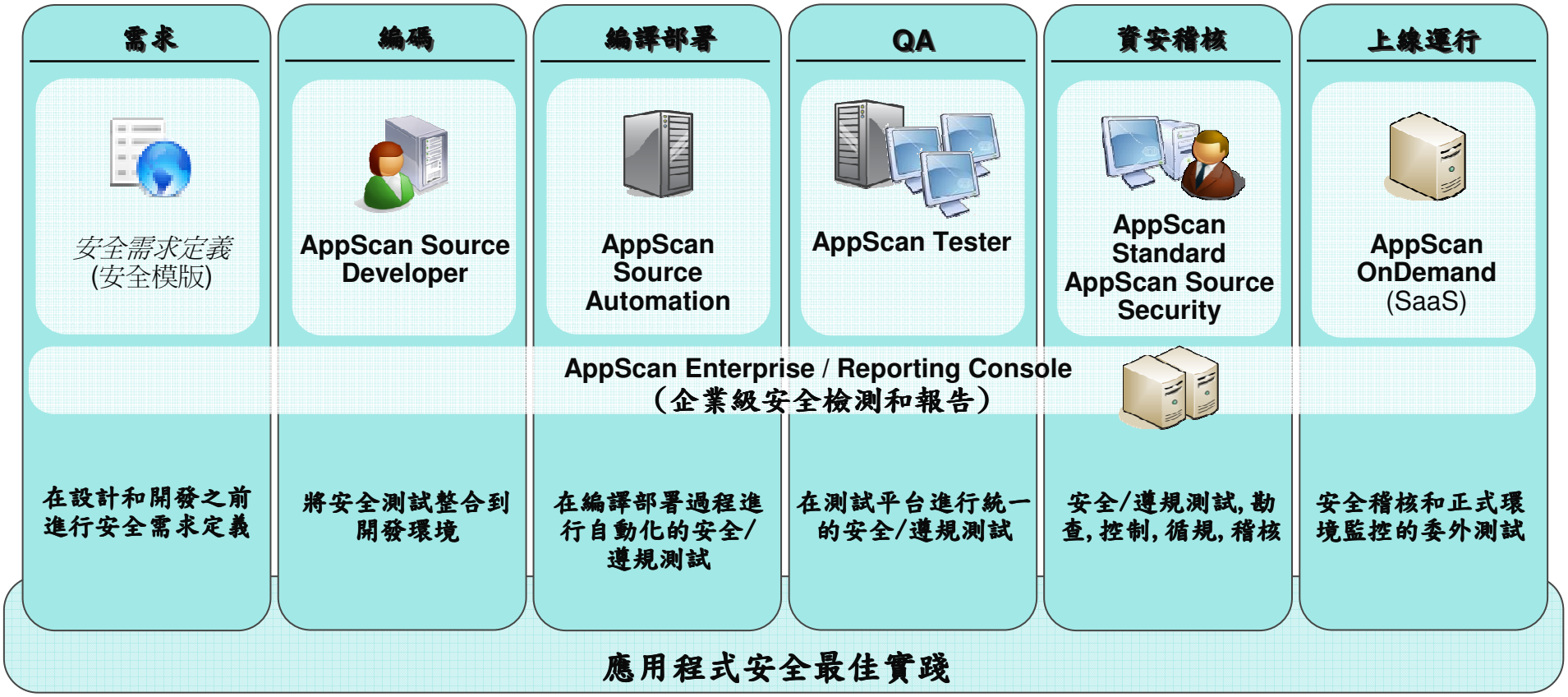
應用程式最危險的地方，或許在於設計人員無法在程式部署完成以前全面掌握其組成成分與安全性，等到程式建置完成後，各種惡意程式與安全弱點可能早已嵌入應用內，任何改變也為時已晚。

案例: Parameter Tampering
可直接讀取其他人的交易內容-授權機制有嚴重漏洞

- 在網址列把reserID改為2001200
  - 成功顯示出其他客戶的交易明細包含正確的E-mail

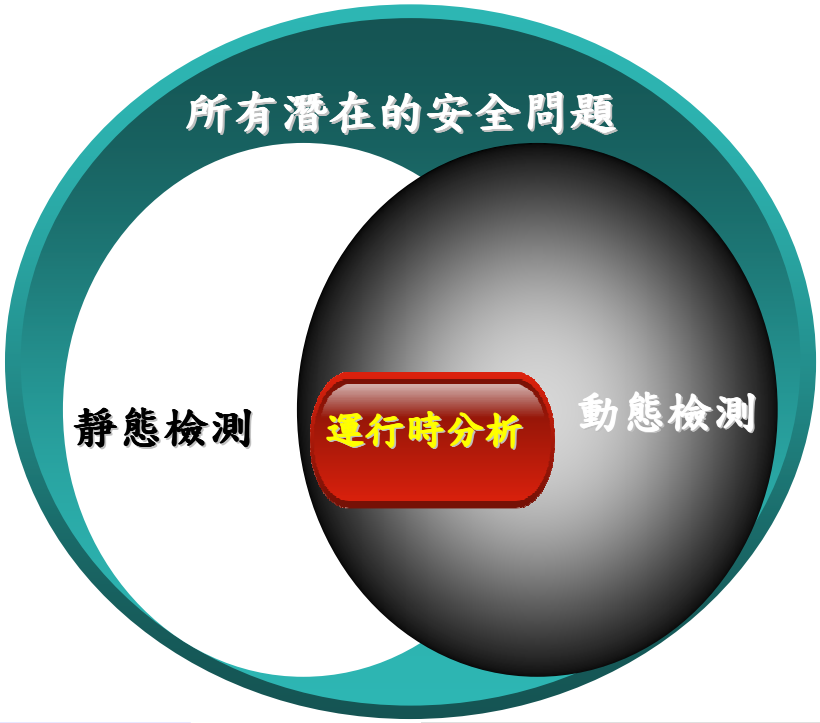
案例: SQL Injection 盜取帳戶資料

因應這些挑戰，安全開發功能須被納入應用開發工具與平台中，才能在開發過程各個階段中執行安全診斷，並將組件掃描（component scanning）融入整合分析（composite analysis）內。組織也應追查軟體系統部署的來源，以確保關鍵應用不受侵害。



Rational AppScan 全面的應用程式安全管理平台，能為軟體開發過程各階段增添應用掃描與安全診斷功能。

- IBM是當今唯一同時具備系統安全動態檢測(黑箱測試)和程式碼安全分析檢測(白箱測試)技術的公司
- 黑箱測試工具由於直接模擬駭客的攻擊，是應用程式安全的基礎設施，應優先考慮。



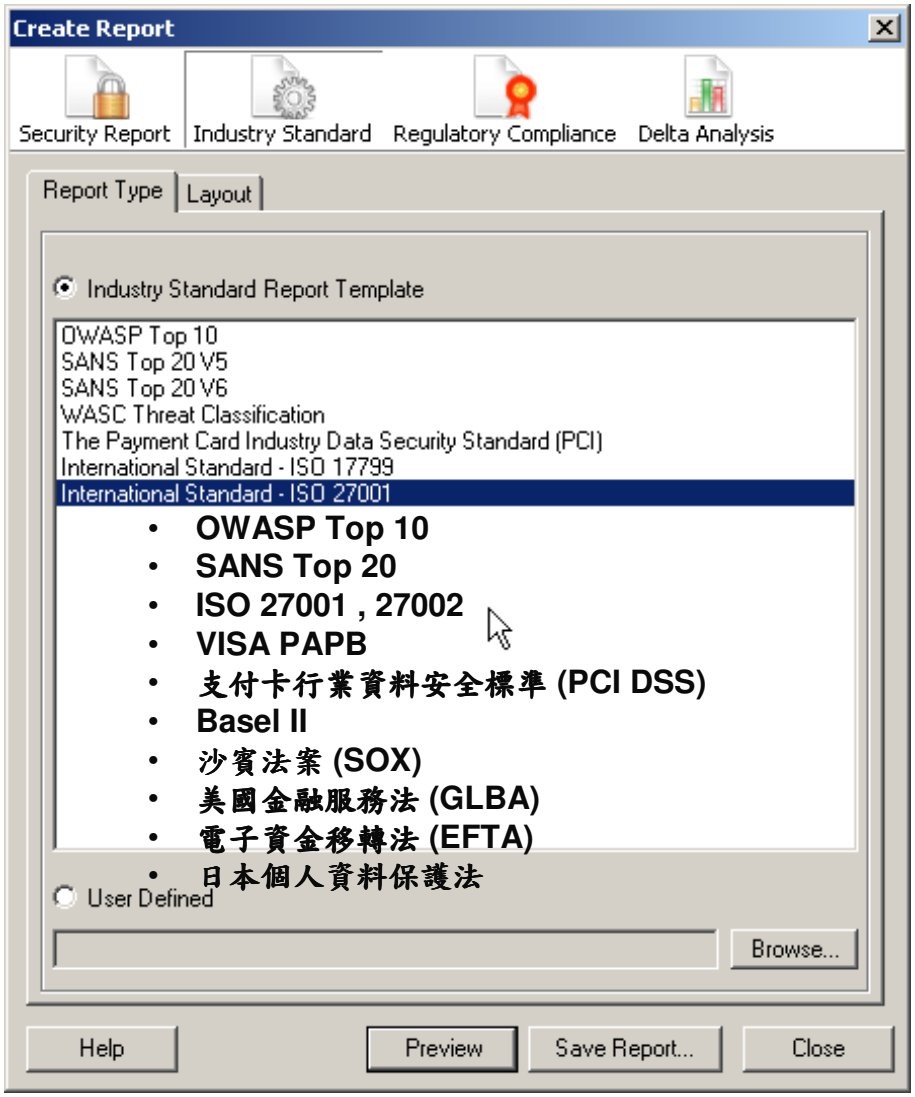
- **WEB應用程式安全檢測——黑箱**
  - 前身為Watchfire公司的產品，產品首見於1996年，**2007年併入IBM**
  - AppScan是業界**最準確**的WEB應用程式安全測試軟體
  - 在應用程式資安弱點評估軟體**市場排名第一**（IDC和Gartner）
  - 全球客戶超過**1000家**
- **程式碼安全檢測——白箱**
  - 前身為Ounce Lab公司的產品，成立於2002年，2009年併入IBM
  - 2009 Gartner's 1st Magic Quadrant稱其為靜態程式碼安全測試業界的"領導者"
  - 程式碼安全分析檢測專家

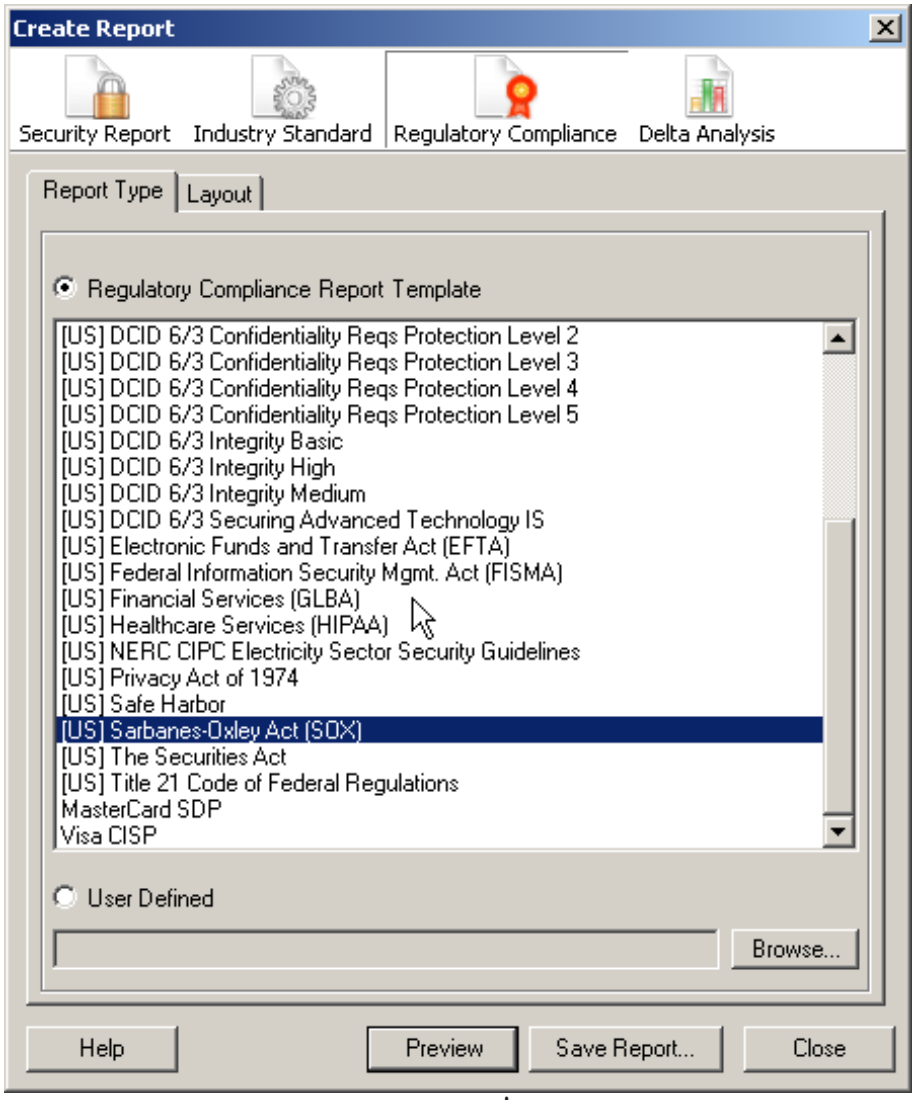
SC MAGAZINE AWARDS 2007 WINNER

JOLT 17th Annual PRODUCT EXCELLENCE AWARD

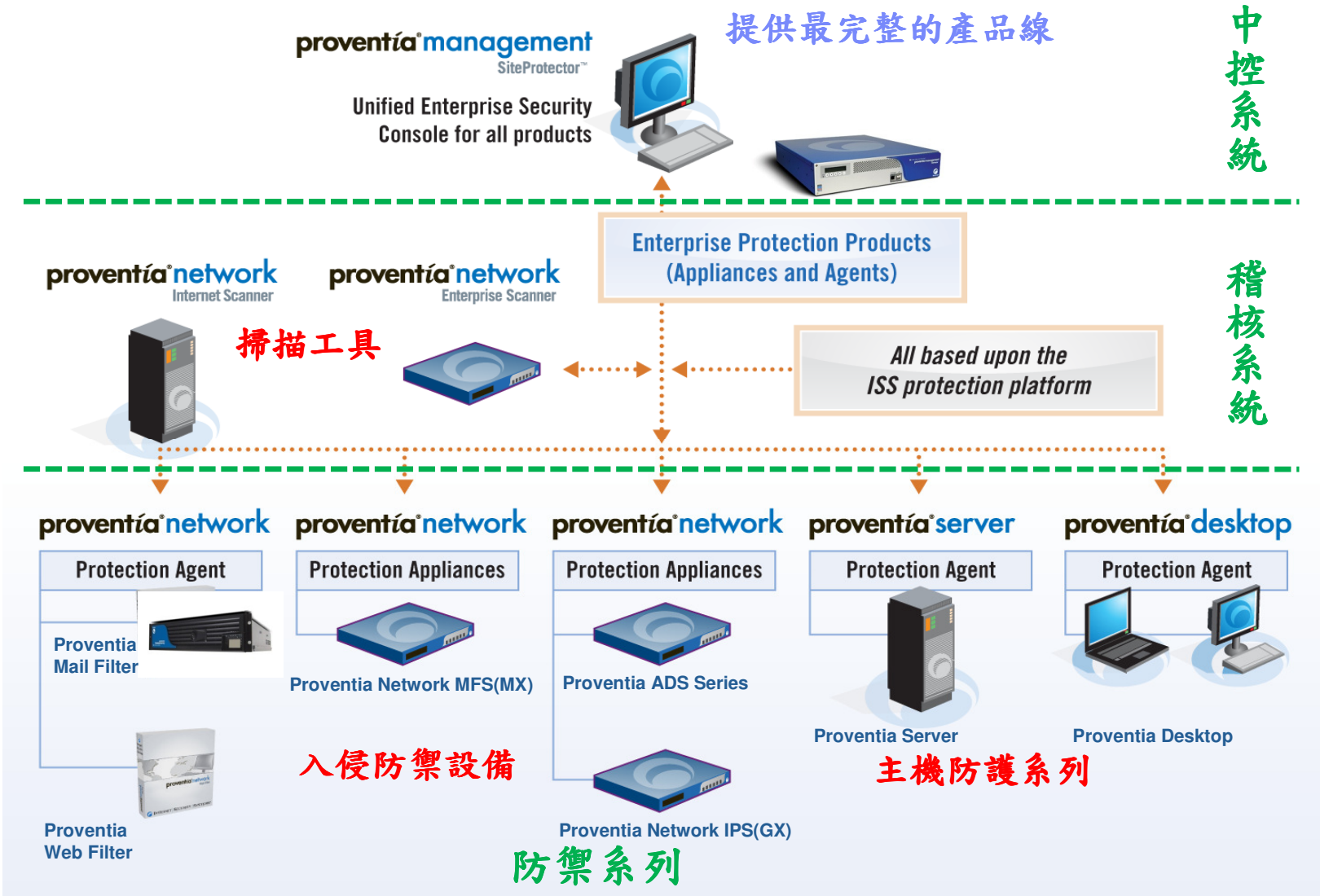
#1 Market Share for Application Security
– Gartner & IDC

內建近50種產業標準、資安法規的報告範本，並將之融入企業應用安全整體分析之中。





傳統的入侵預防系統與防火牆技術已不足因應駭客攻擊，企業需以融合整合式網絡、伺服器保護技術，在 IBM ISS網路安全防護方案的策略架構，結合網路入侵防禦設備及掃描公具、主機防護系統並整合稽核及中控系統功能，才能克服這些不斷演變的安全挑戰。



建構企業安全平臺－展現”無故意或過失責任“的免責

Cost Efficient and Flexible Pricing Model

- 綜合4個關鍵環節+2類安全服務+1個統一安全管理平臺
- 輕鬆實現前瞻動態威脅保護

何必花錢買昂貴的Web Application Firewall ？
IBM IPS功能增強－Web Application Protection

- 在原有IPS功能的基礎上增加應用層防火牆：
  - SQL (Structured Query Language) Injection
  - LDAP (Lightweight Directory Access Protocol) injection
  - XSS (Cross-site scripting)
  - HTTP (Hypertext Transfer Protocol) response splitting
  - JSON (JavaScript Object Notation) hijacking
  - PHP (Hypertext Preprocessor) file-includes
  - CSRF (Cross-site request forgery)

- **IBM IPS擴展PCI-DSS的覆蓋範圍包括：**

  –Payment Card Industry (PCI) Requirement 6.6 which goes into effect on .

  6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

  - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.
  - Installing an application layer firewall in front of web-facing applications.

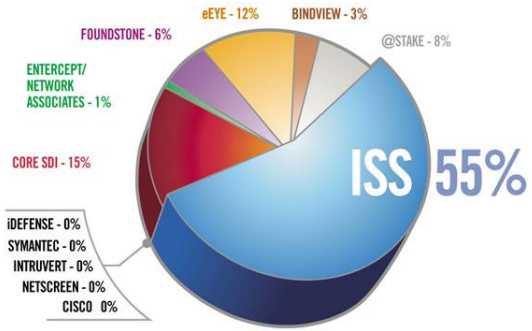
Proventia G200

Proventia intrusion prevention appliances

在IBM ISS X-Force® 研發團隊的支援下，於全球擁有多座資安研發實驗室及安全監控中心(SOC)

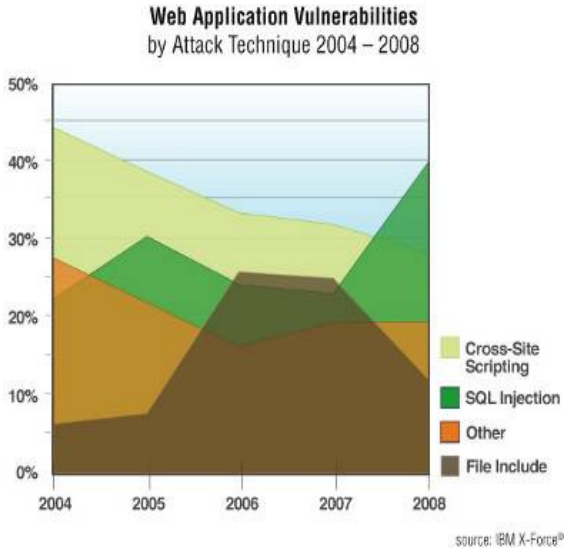
X-Force 是全球頂尖的企業級安全研發團隊

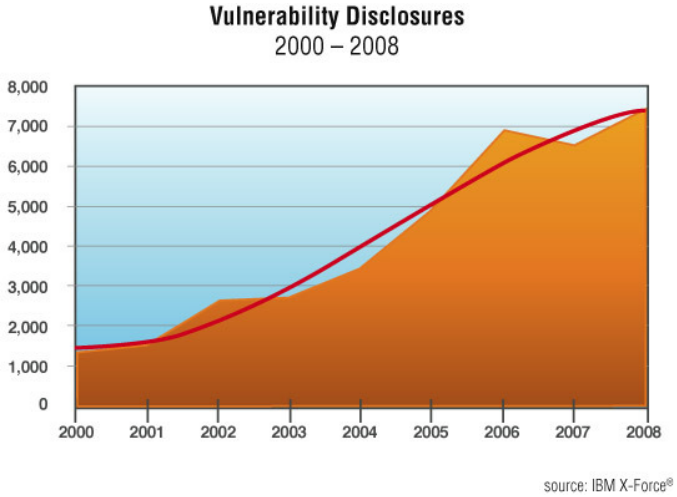
- 長達14年的研發歷史
- 專注于發現和分析安全風險，開發技術對策
- 每半年發佈一次網路整體風險趨勢狀態報告
- 每年發佈30 次以上的安全建議和警告
- 每月找出200 多個新的攻擊手法
- 維護超過 38,000 個漏洞的安全資料庫
- 開發了 6000 多個檢查項用於檢測和發現攻擊手法
- 發佈X-Force月度威脅觀察報告 (XFTIM)
- 2008年，研究與發現7406個安全漏洞
- CVE組織創始人之一，相容CVE/CPE/CVSS

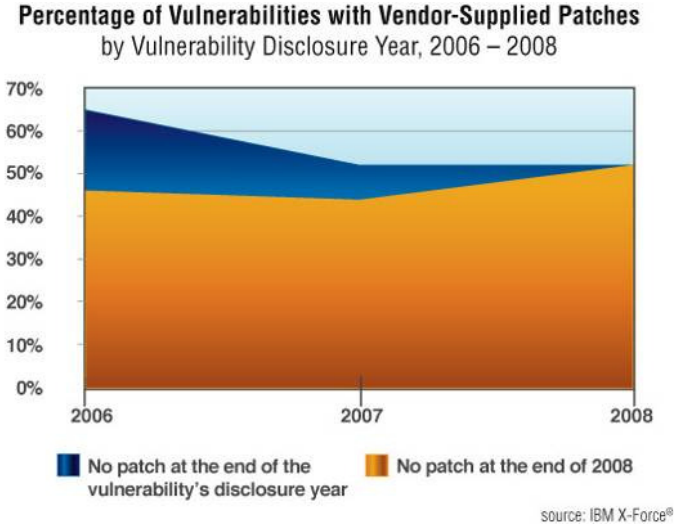


高風險漏洞發現比例

Frost & Sullivan 2006 , Internet







A Smarter Planet

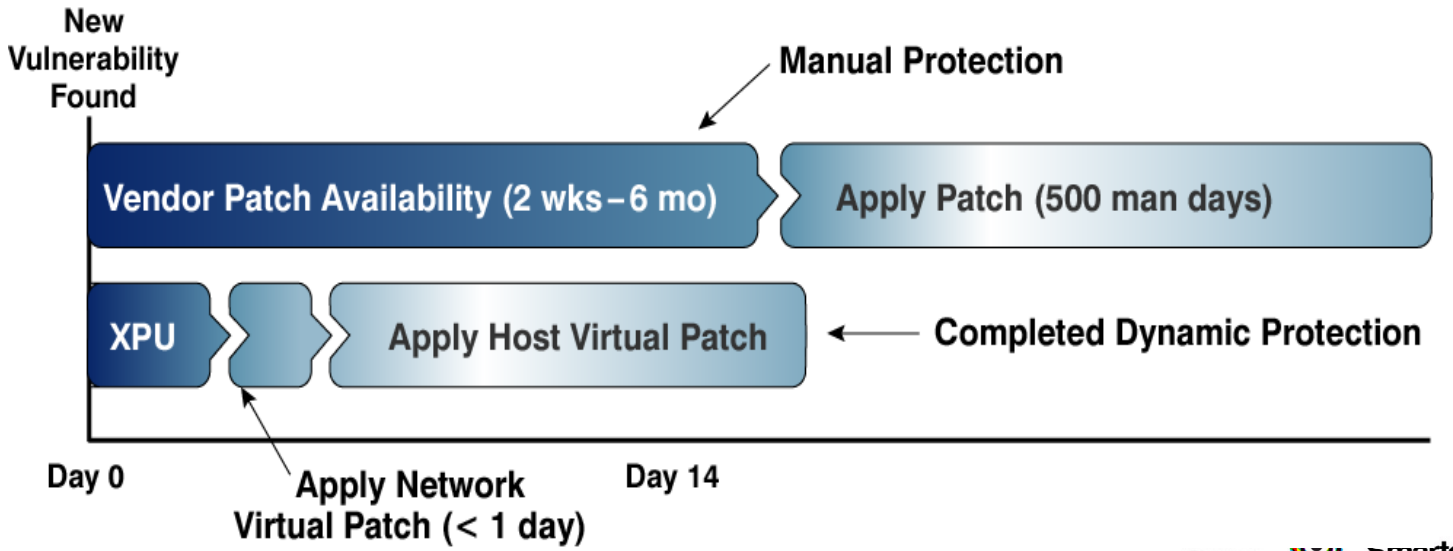
SmarterSecurity&Resilience

IBM ISS 核心價值- Virtual Patch 虛擬補丁

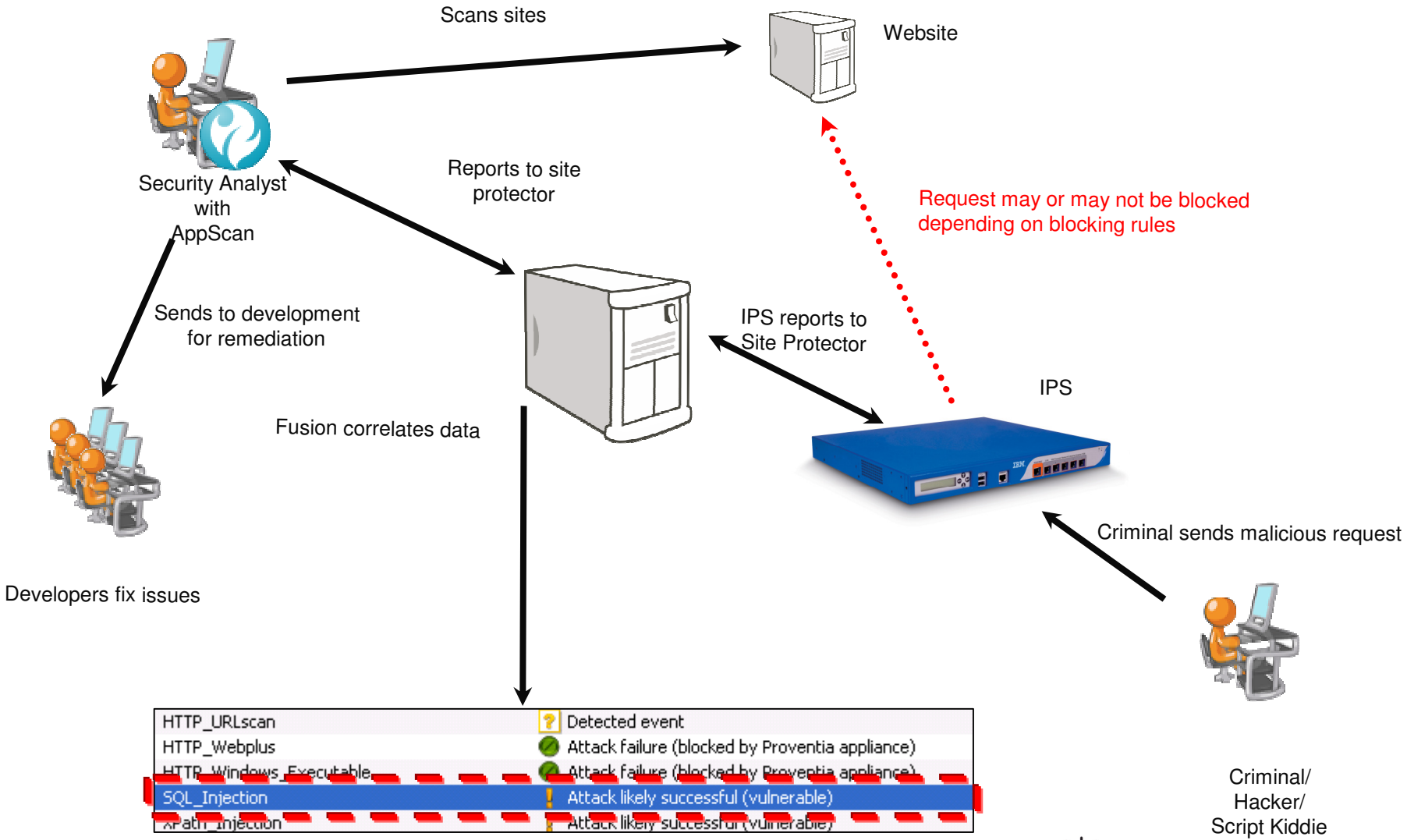
Virtual Patch 為面臨最新漏洞威脅的企業提供了充分的 時間緩衝 ，在系統和應用廠商就新漏洞提供補丁和更新之前，防止漏洞被利用，同時也可避免補丁與業務應用衝突的風險，確保企業的安全。

為什麼能夠實現前瞻性保護？（Proactive Protection）

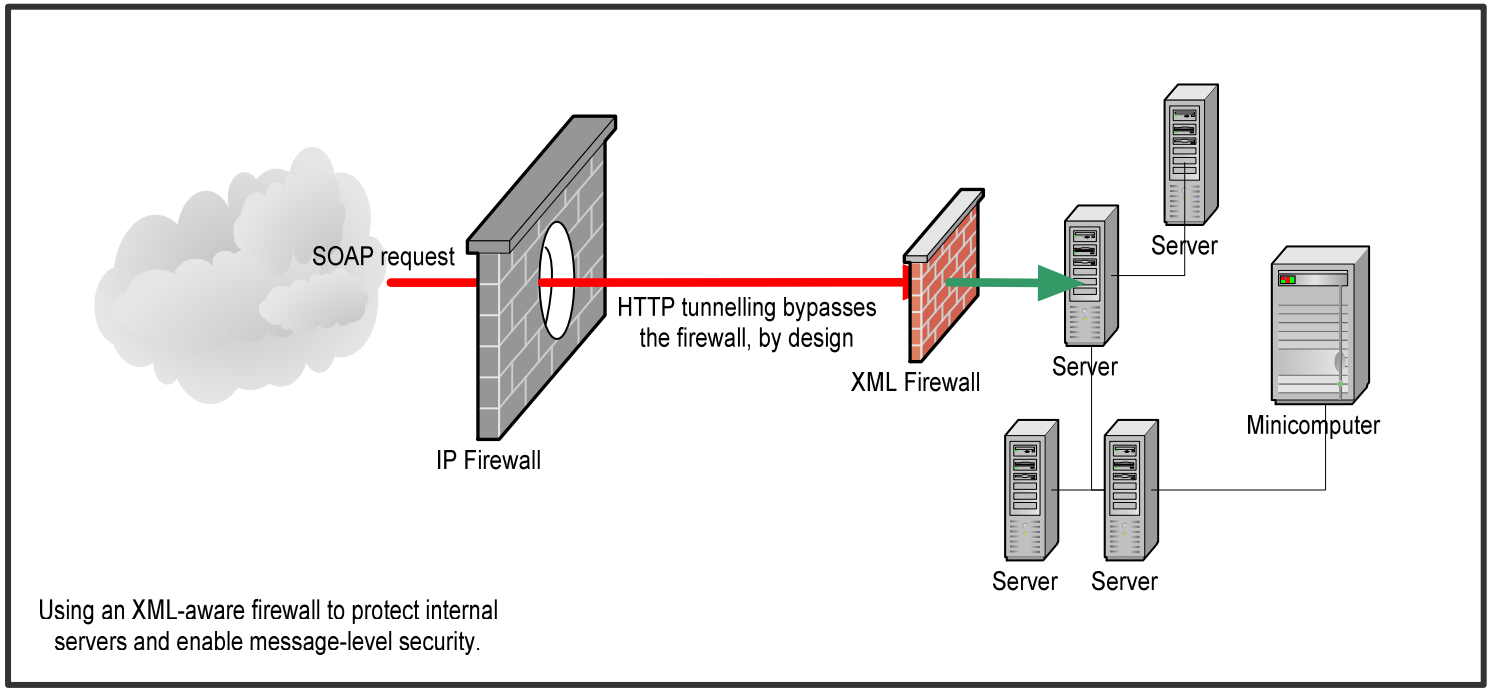
由於IBM ISS首先發現的高危漏洞最多，同時，和系統廠商保持了雙贏的合作關係，所以有能力在漏洞被發現的第一時間提供針對漏洞本身的防護，而非提供針對攻擊的防護。因此，無論攻擊手法和利用程式如何變化，ISS提供針對高危漏洞的前瞻防護。



IBM AppScan 與 ISS 完美的結合：應用程式安全檢測與網路安全防護的整合



在XML/Web Service 應用中，WebSphere DataPower SOA Appliances可保護應用程式不受未經授權存取與惡意訊息的侵害，提供完整的安全資料交換機制。

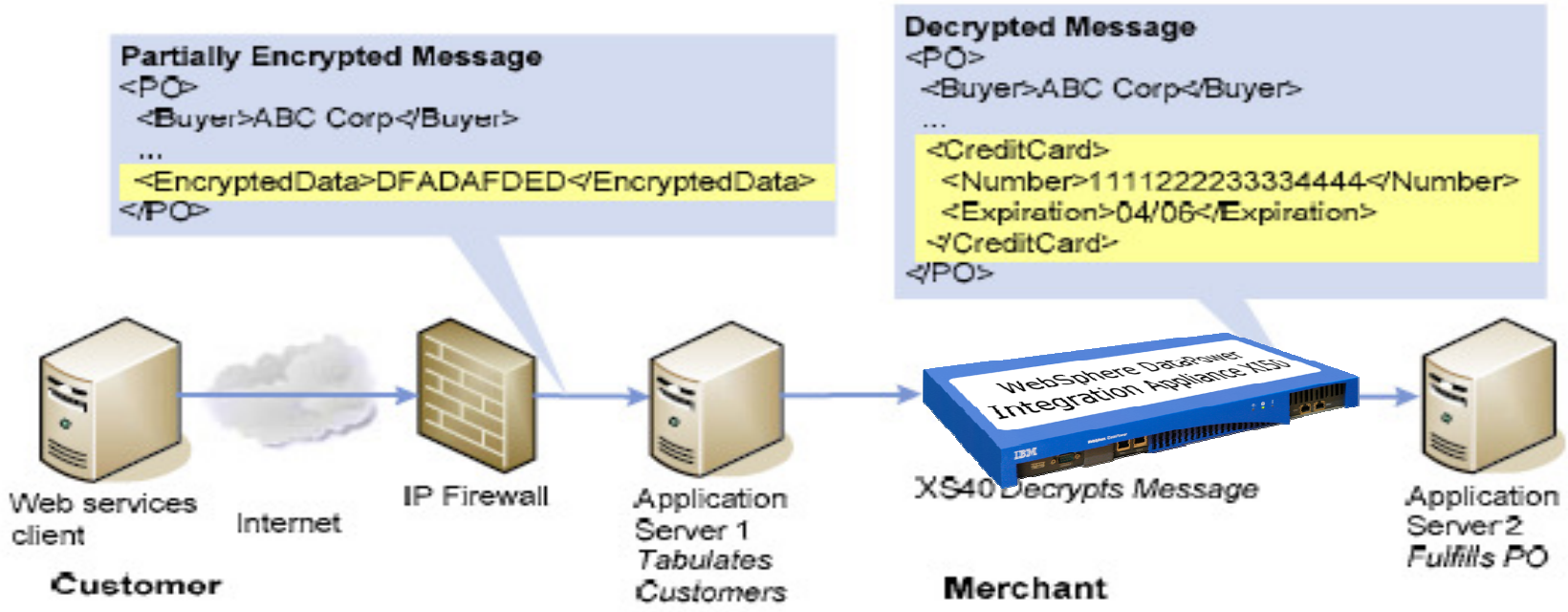


- 應用設備達到最高安全等級
- 應用設備加速加解密速度
- 支援高等級的加密演算法
  - –Encryption algorithms: 3DES, DES, AES
- 較低的TCO 與最佳 ROI

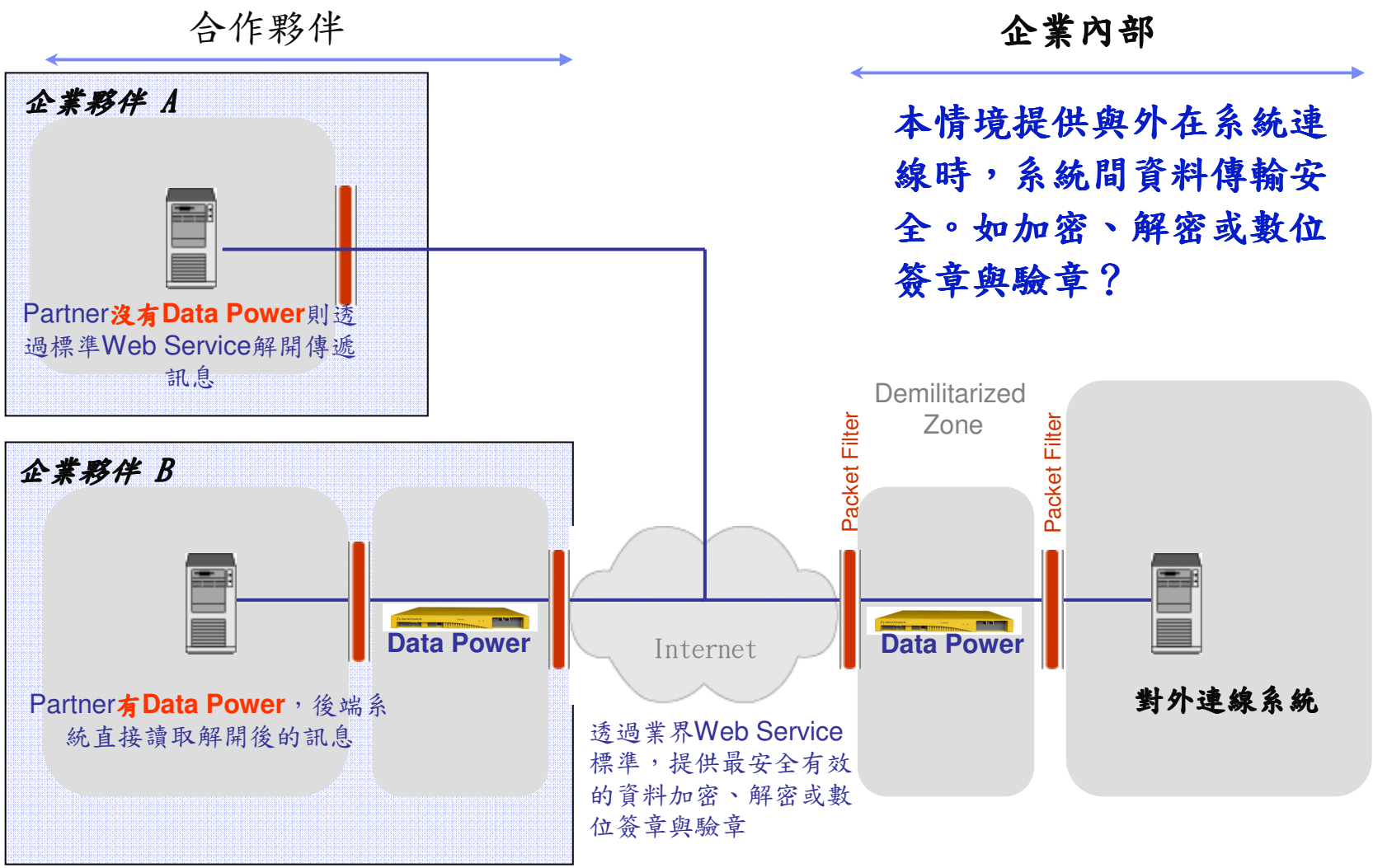
WebSphere DataPower SOA Appliances – XML Firewall 加/解密技術示意圖

XML Security Gateway

–Data encryption and decryption between external clients and internal Web services servers.



WebSphere DataPower SOA Appliances使用案例與情境：
與外界系統之間資料交換安全案例



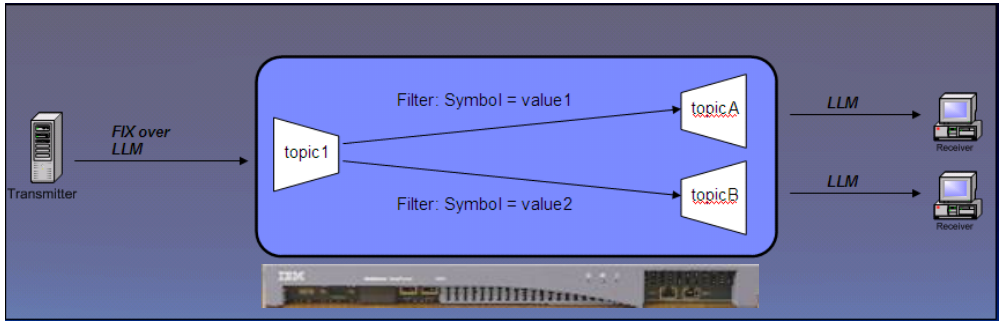
WebSphere DataPower SOA Appliances使用案例與情境：
金流訊息 (FXML)交換平台

目標產業 – 金融服務業

目標客戶(群) – 銀行, 證券

解決方案目的與功能描述

隨著年底臺灣正式大規模採用XBRL財報平台，面對國際化的XML資訊交換趨勢，是銀行迎向全球供應鏈提昇業務的重要時刻，此時更需要在調整作業模式的階段，跨足FXML金流訊息交換平導入兼具效能與效率的系統，才能夠從瞬息萬變的市場中，直跑在競爭對手的前方！



對客戶的好處

- 可介接安控機制，負責FXML訊息傳送過程之加解密
- 保證完成FXML訊息所指定之交易流程(Guarantee Delivery)
- 可與ICP、財金公司、中心廠/供應商之跨行交易

相關的IBM軟體:

WebSphere DataPower XM70+MQLLM

客戶價值分析:

IBM：硬體解決方案的領導者

本地廠商：無法提供可與IBM比擬的完整硬體解決方案與整合藍圖

預估實施所需時程與次序:

3～8 個月（需求分析、教育訓練、系統設計、系統建置及客製、上線教育訓練、測試上線）

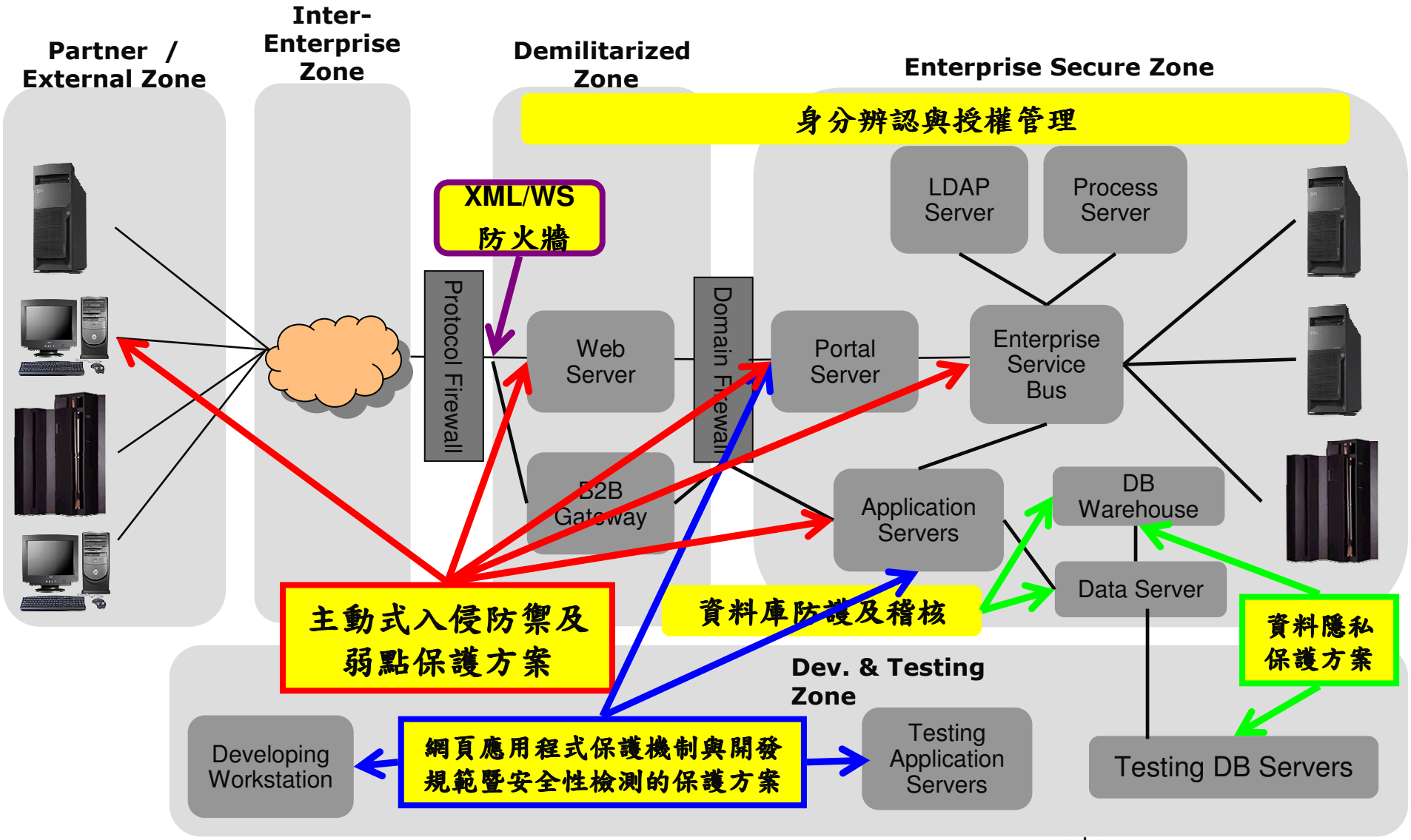
成功案例 References

客戶證言 「導入 DataPower後，處理速率就明顯改善，現在處理過去兩、三倍的資料量都沒問題：其次，DataPower可協助在訂單資料進來及出去前先進行XML的格式驗證，一旦錯誤就直接擋信，此一驗證讓資料量大的公司可節省人力成本。」 **～宏碁集團資訊技術總處 資訊長 李文進**

專案效益

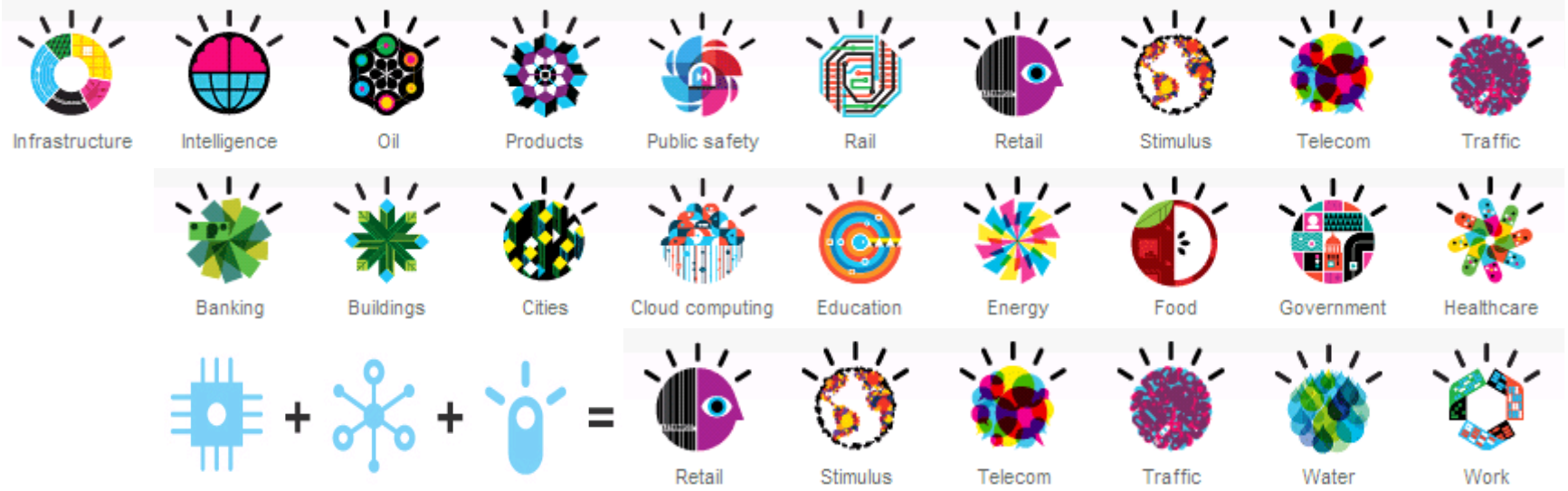
1. 大幅增加系統整合與開發的生產力
2. 減少系統開發、測試時間、專案建置風險與導入期間並減少系統上市時機
3. 增加系統處理效率與系統處理資料量二~三倍
4. 增加擴充性和穩定性

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



Q & A

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



IBM Global Services
3-4F, No.7, Song Ren Road,
Taipei, Taiwan

Produced in Taiwan

Steven Chuang, FSS Solution Team, IBM Taiwan
0933-205-029
chsteven@tw.ibm.com