雲計算模式下的安全和駭客經濟威脅趨勢

萬濤 ChinaEagle

IDF互聯網威懾防禦實驗室
中國電子學會計算機取證專家委員會

智慧的地球對安全的需求

這個星球變得越來越...

- 機械化,
- 互聯 化
- 智能.化

新的成為可能
新的複雜性
新的風險.

“我們在過去十年中看到的變化比再之前90年的總和都要多”

Ad J. Scheepbouwer, CEO, KPN Telecom

Infrastructure and application protection	Privacy and identity controls	Information protection and recovery	Governance and policy management

中國，僵屍電腦第一生產大國

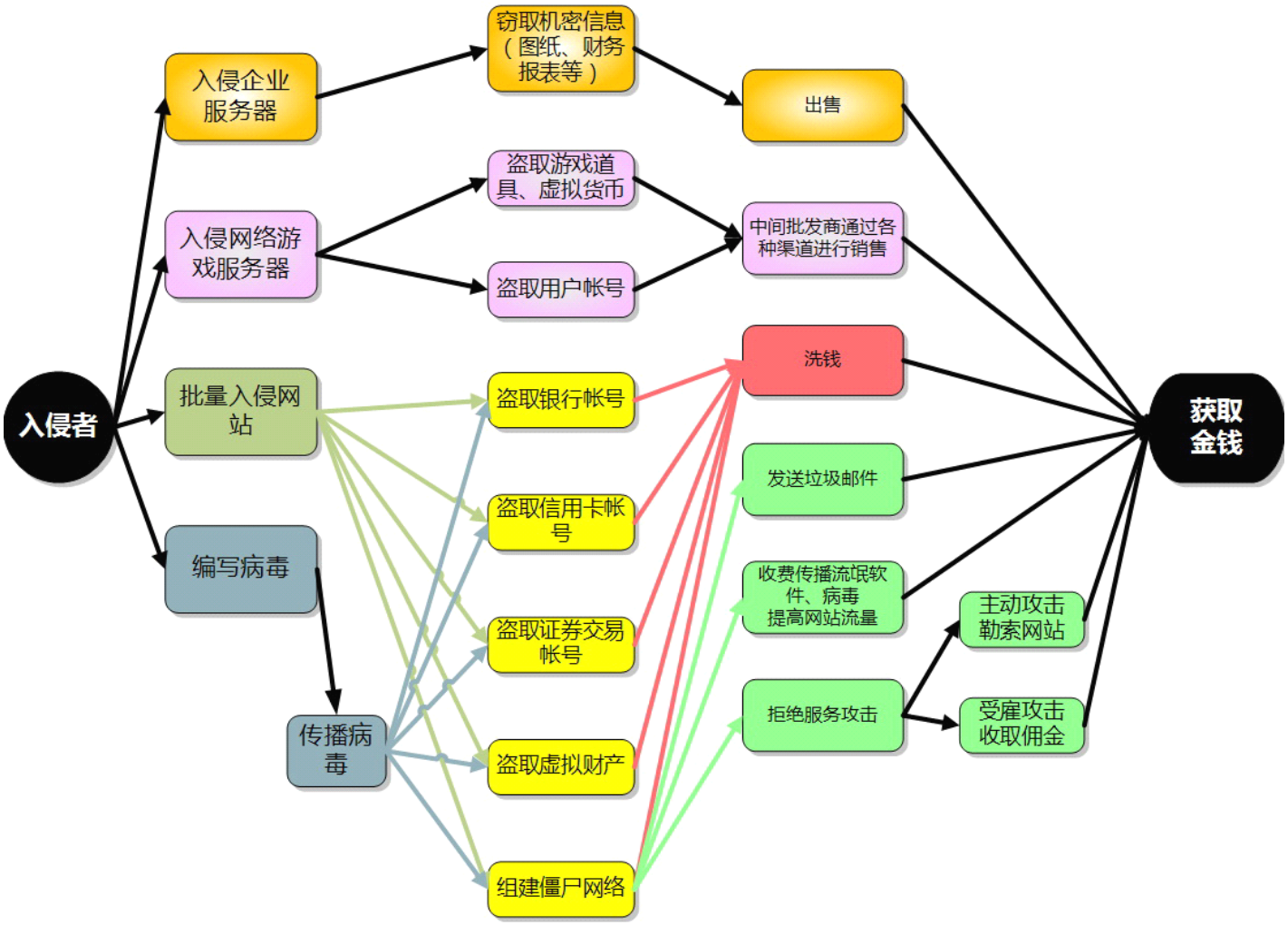
出产僵尸计算机的前 10 个国家 / 地区

2009 年第四季度		2009 年第三季度		2009 年第二季度	
国家 / 地区	占总量的百分比	国家 / 地区	占总量的百分比	国家 / 地区	占总量的百分比
中国	12.0	美国	13.1	美国	15.7
美国	9.5	中国	12.2	中国	9.3
巴西	8.5	巴西	8.0	巴西	8.2
俄罗斯	7.0	德国	7.3	俄罗斯	5.6
德国	6.0	韩国	5.1	德国	5.3
韩国	5.0	意大利	4.3	意大利	4.0
意大利	3.5	印度	3.4	韩国	3.8
英国	3.2	俄罗斯	3.0	印度	3.2
中国台湾	3.0	英国	2.9	英国	3.0
西班牙	2.6	西班牙	2.6	西班牙	2.6
总计	60.3	总计	61.9	总计	60.7

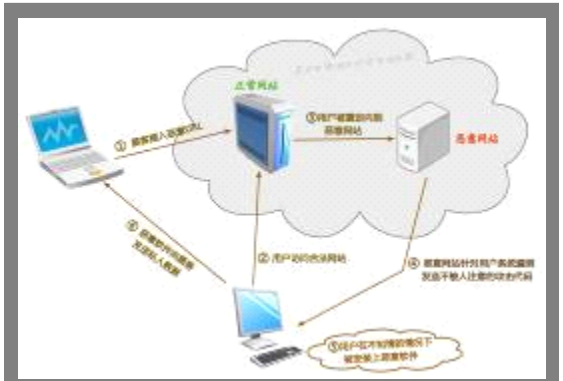
數據來源：邁克菲威脅報告

- 網頁掛馬帶來的最直接後果——“僵屍”如瘟疫般蔓延
- 美國僵屍生產力下降，而中國保持穩步增長，已佔據了生產僵屍電腦第一大國的位置

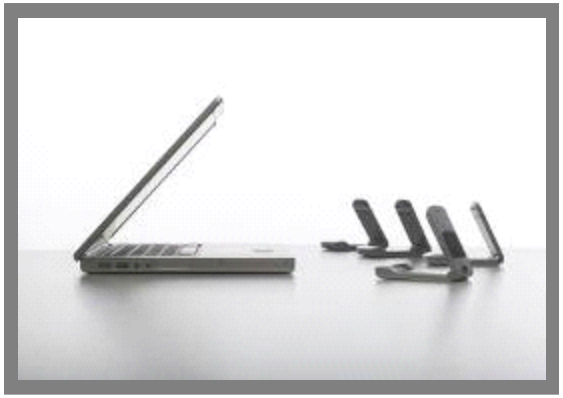
"駭客經濟"模式已基本形成,規模龐大,日趨複雜



威脅發展特點



- 攻擊產業化，威脅數量激增
- 攻擊自動化，快速蔓延
- 攻擊智能化，威脅技術多樣化



- 威脅端到端，依靠單安全組件如何應對？
- 如何做到全方位立體防護？

智慧的地球面臨安全的挑戰

安全專案的核心驅動力

複雜性增加

很快連接在網路上的設備將超過1萬億臺, 組成一個“Internet事務”

成本增加

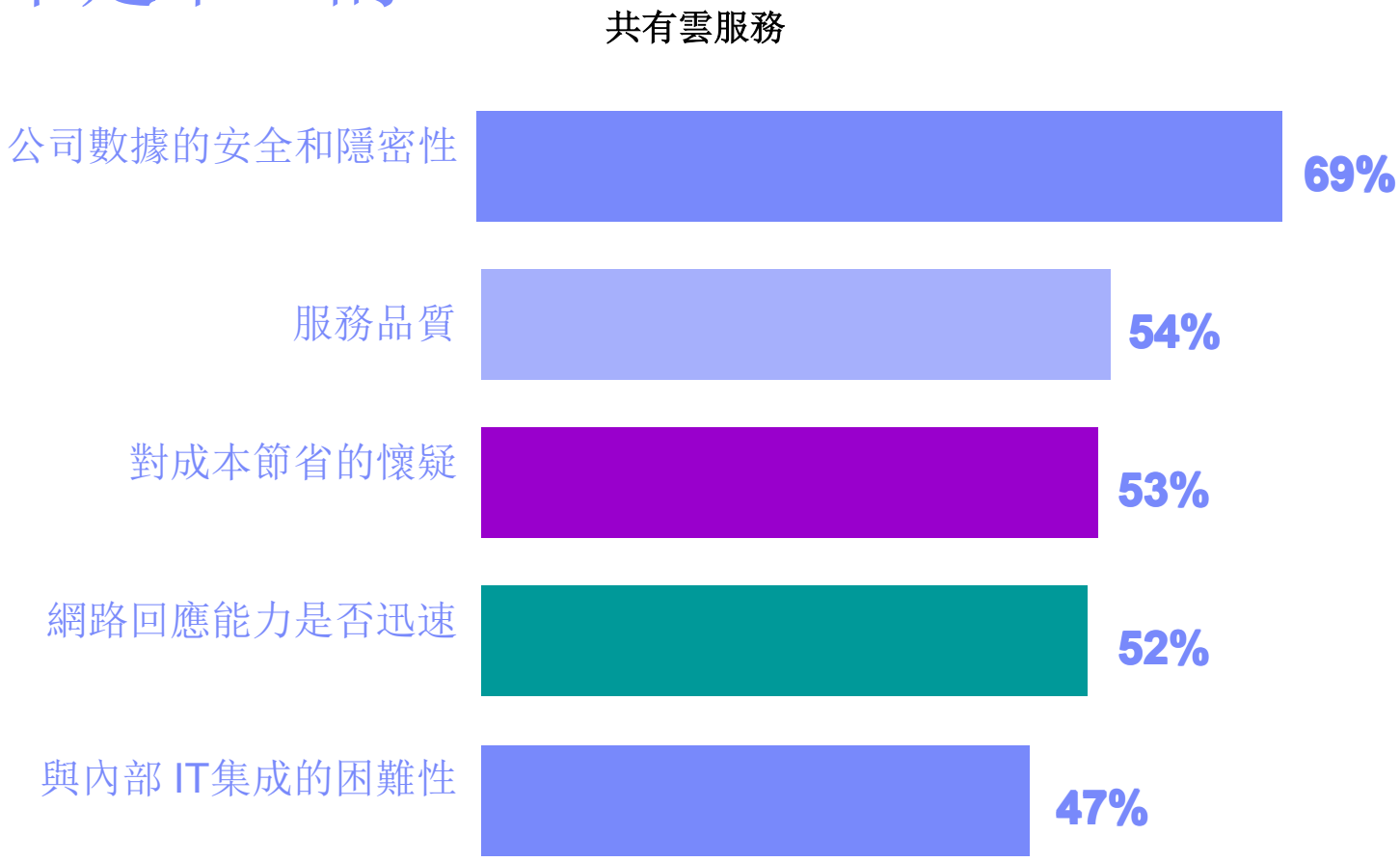
僅僅統計了美國的公司在2010年中用於風險治理和合規的花肥超過了290億美金

合規性要求

保護每一個客戶記錄需要204美元

Source http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

對數據安全和私密性保護的擔心是最主要的 – 但並不是唯一的



Source: Cloud Market Insights, *Cloud Computing Research*, July 2009. n=1,090

特殊用戶對雲計算安全的擔憂

保護知識產權和數據	30%
合規性的能力	21%
非授權使用數據	15%
數據機密性	12%
數據可用性	9%
數據完整性	8%
可以測試和審計供應商的環境	6%
其他	3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

現在是換個思路考慮安全的時候了

從設計就開始考慮產品和服務的安全性

安全要適應新興的技術和商業模式

雲的屬性極大地影響資訊安全

內部實施 → 外部實施

單層租賃 → 多層租賃

IT服務 → 自服務

慢供應 → 快速供應

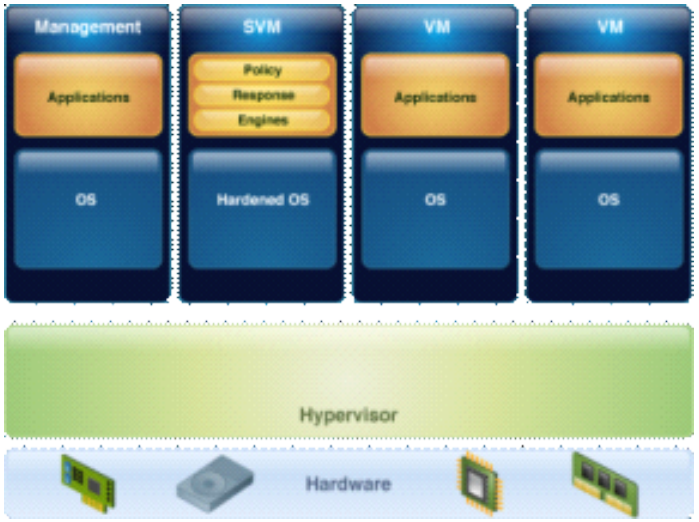
虛擬化所帶來的安全複雜性

- 新的複雜性
  - –動態地重新分配VM
  - –增加的架構層來管理和保護
  - –一個物理伺服器上有多種操作系統和應用
  - –系統之間取消了物理的隔閡
  - –手動地跟蹤軟體和配置 VMs

虛擬化之前

- 1:1 OS和服務在一個物理機上

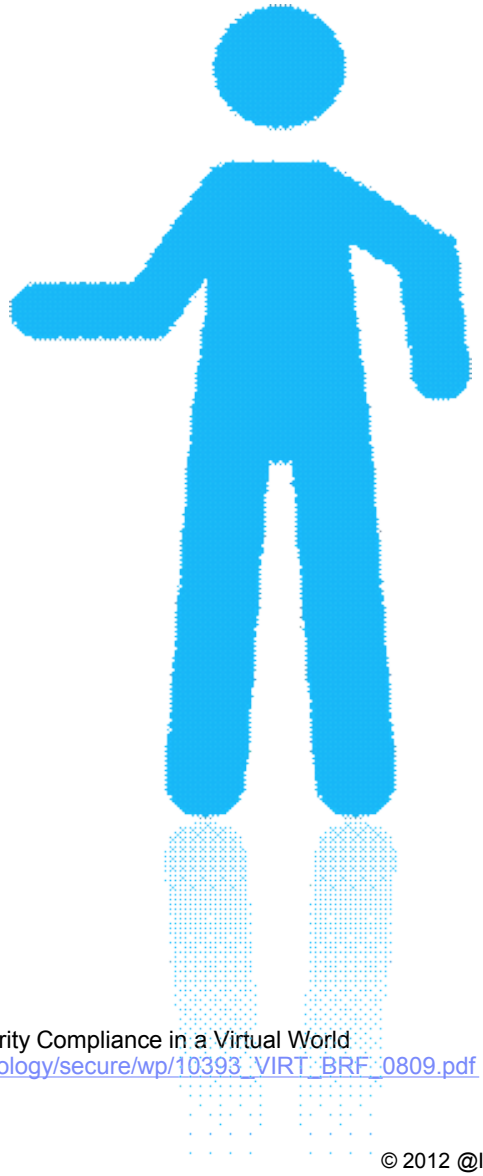
虛擬化之後



- 1:多 操作系統和服務在一個物理機上
- 多出來一層來進行管理和保護

在虛擬化環境下安全合規的最佳實踐

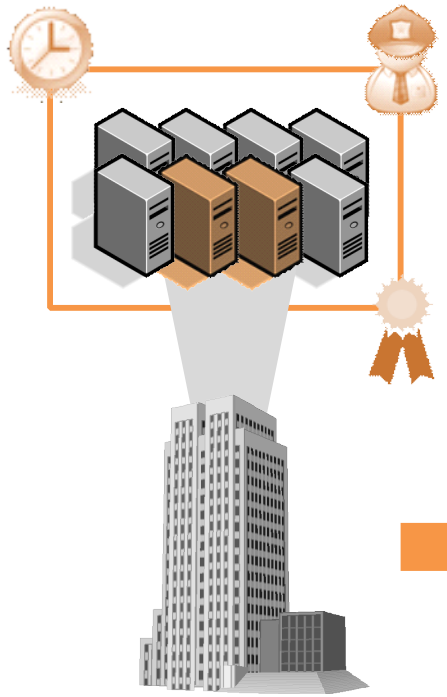
- 變更和配置流程需要按照虛擬化的框架來進行擴展：
  - 在動態的環境下管理員增加的了成本和複雜性
  - 確保不定管理延伸到虛擬環境中
- 在高度整合的情況下保持獨立訪問控制
- 提供虛擬伺服器和虛擬網路的安全分段
- 維護虛擬審計日誌



*Source: RSA Security Brief: Security Compliance in a Virtual World
http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf

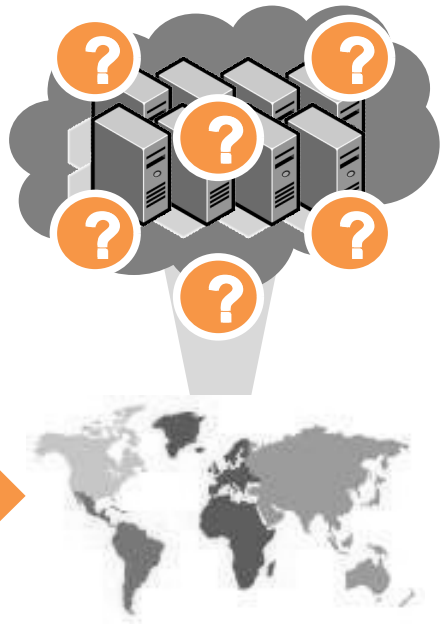
雲計算安全：簡單的例子

今天的數據中心



我們控制
它位於 X.
塔被存儲在伺服器Y, Z.
我們有備份
我們的管理員控制訪問.
我們的線上時間足夠
審計員高興.
我們的安全團隊被引入.

明天的雲



誰能控制
它位於那裏?
它存儲在那裏?
誰來備份?
誰來訪問?
是否有足夠的彈性?
審計員如何評論?
安全團隊如何引入?

雲計算風險類別

很少的控制

客戶期望對系統進行有效管理

可靠性

數據中心的高可用性尤其重要

數據安全

在共用的網路和數據中心，數據訪問控制尤其重要

合規

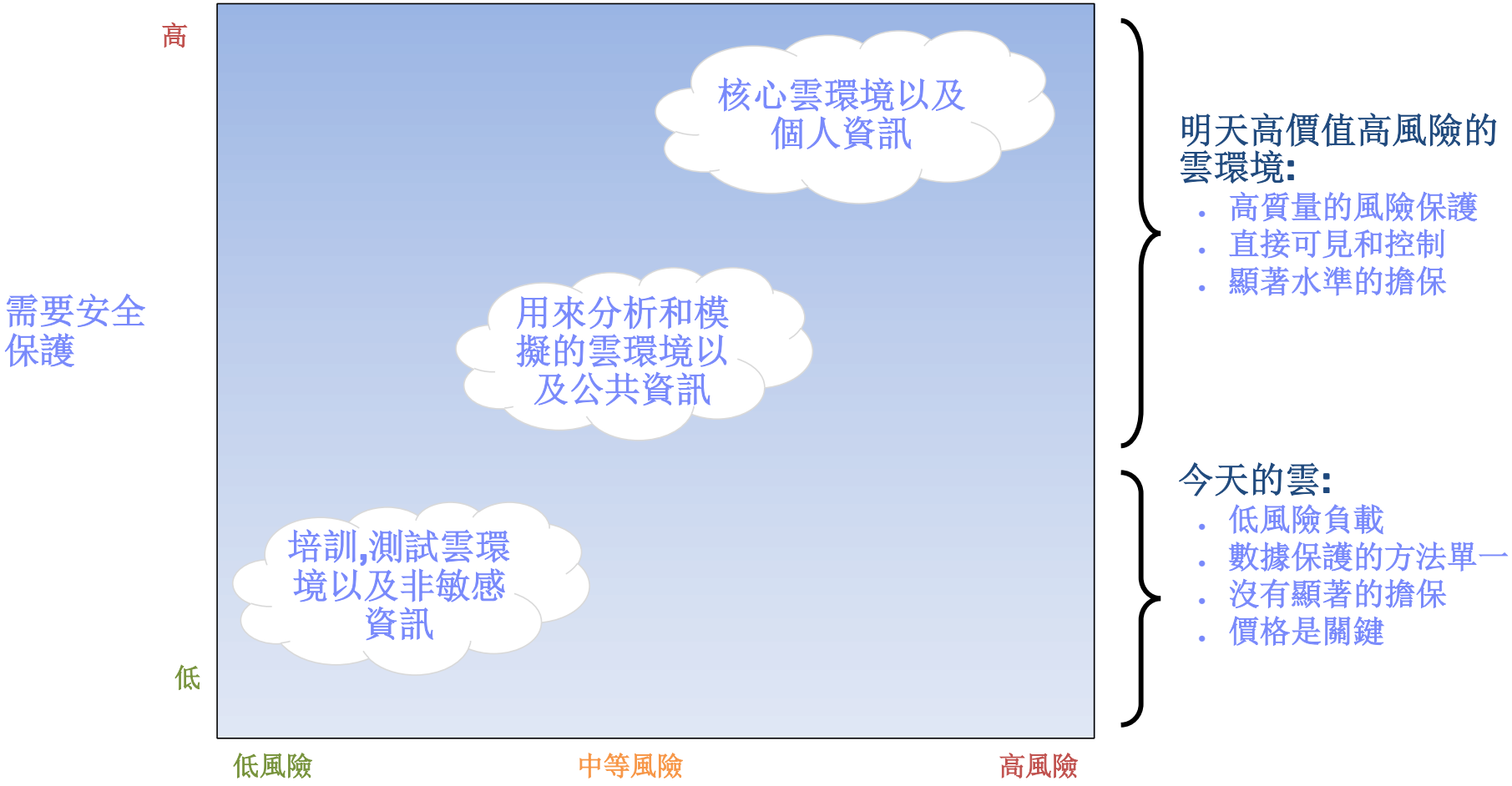
SOX, HIPAA 等合規要求

安全管理

應用和錯作系統的安全設置和管理

一人難稱百人意

不同的雲環境有不同的安全風險



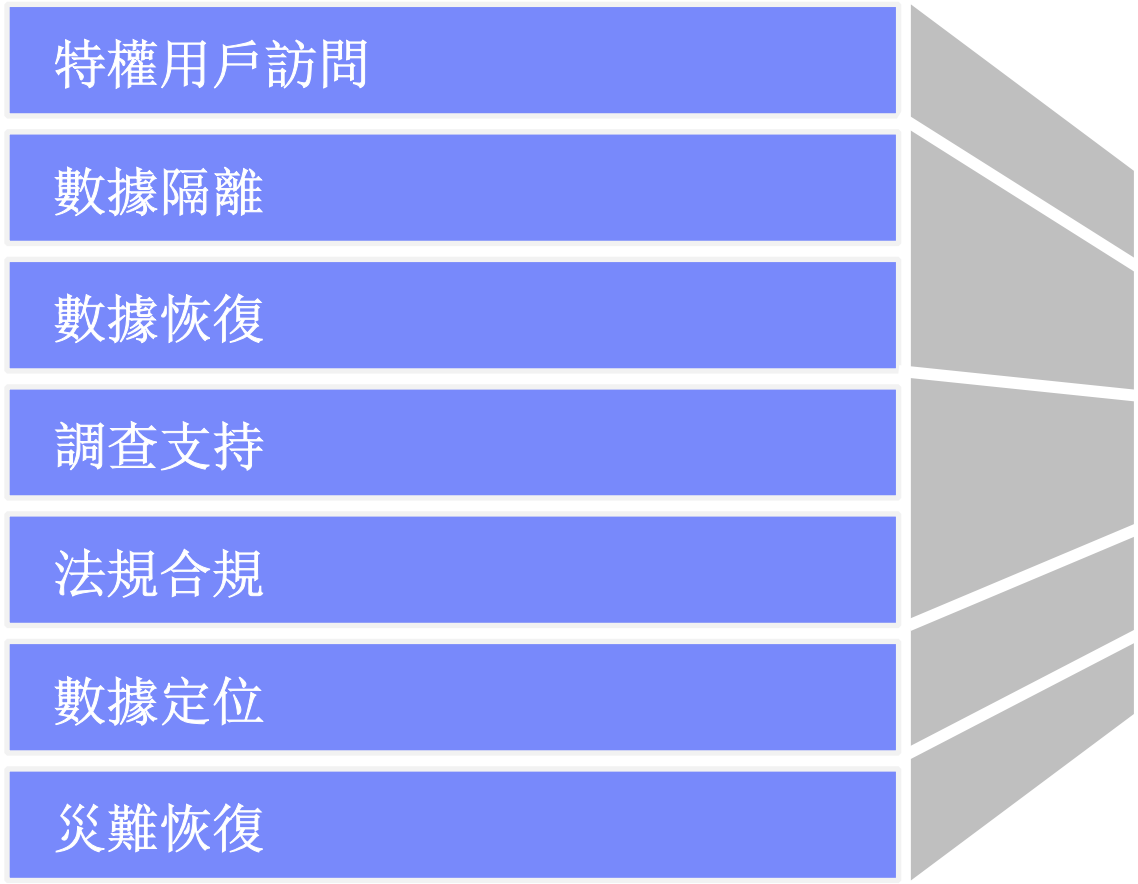
明天高價值高風險的雲環境:

- 高質量的風險保護
- 直接可見和控制
- 顯著水準的擔保

今天的雲:

- 低風險負載
- 數據保護的方法單一
- 沒有顯著的擔保
- 價格是關鍵

Gartner的雲計算安全風險分析



Gartner: Assessing the Security Risks of Cloud Computing, June 2008

Cloud Security Framework

Cloud Security Guidance Document

Security Products and Services

安全監管，風險管理和合規

客戶需要清晰的瞭解他們的雲安全狀態

實施監管和審計的管理程式

- 建立第三方審計 (SAS 70, ISO27001, PCI)
- 提供使用者日誌和審計數據訪問
- 建立有效的使用者事故報告機制
- 可視化的變化，事故和映像管理等
- 支持電子數據取證和發現

可用的產品，服務和解決方案

Cloud Security Risk Assessment

創建路線路來評估安全和減少風險

全面的評估機構現有的安全策略，過程，控制和機制評估。

Cloud Resiliency Consulting Services

評估和計畫 – 彈性的雲驗證

全面的評估機構現有的災難恢復計畫及與環境的一致性。

Cloud Security Framework

Cloud Cloud Security Guidance Document

Cloud Security Products and Services

人員和身份

客戶需要雲提供嚴格的身份驗證

實施增強的身份和訪問控制

特權用戶監視，包括日誌活動，物理監視和背景檢查
利用聯合身份，協調與企業或第三方體系認證和授權
一個以基於標準的單點登錄功能可以幫助簡化用戶對內部託管程式和雲的登錄
生物識別技術改變傳統帳戶密碼模式

可用的產品，服務和解決方案

Federated Identity Manager

雲身份安全管理

採用用戶中心聯合身份管理，提高客戶滿意度和合作能力

Security Information and Event Manager

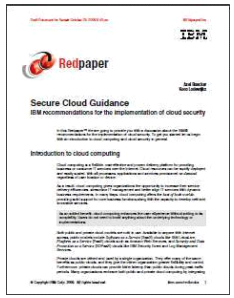
優化安全和合規工作

監視可能導致資訊風險的用戶偶然或惡意的行為

Cloud Security Framework

數據和資訊

客戶最關心的就是數據安全



Cloud Cloud Security Guidance Document

確保機密資訊的安全

- 使用安全的網路協議時，連接到安全的資訊存儲。
- 採用防火牆來隔離機密資訊，並確保所有機密資訊存儲在防火牆後面。
- 業務無關的敏感資訊應該安全的銷毀

Cloud Security Products and Services

可用的Cloud產品，服務和解決方案

Cloud Data Security Services

保護數據支持商業創新

提供防止網路數據丟失，端點加密，防止終端數據丟失和日誌分析的方案

Cloud Information Protection Services

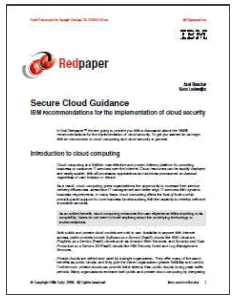
持續的數據保護

- 遠程數據保護服務
- 電子郵件敏捷管理
- 線上的快速保護

Cloud Security Framework

應用程式和過程

客戶需要安全的雲應用程式和供應流程 .



Cloud Cloud Security Guidance Document

建立應用程式和環境配置

- 實施應用管理和映像提供程式.
- 實施安全應用測試計畫
- 確保所有的虛擬映像和應用程式的修改都進行記錄.
- 為所有的web應用開發使用安全編碼指南

Cloud Security Products and Services

可用的Cloud產品，服務和解決方案

Cloud AppScan/WAF

Web應用程式的安全漏洞測試與保護

提供具有可擴展的企業架構，可集中並行掃描或保護多個應用程式的解決方案。

Cloud XML Security Gateway

代碼級的面向Web的應用程式安全漏洞解決方案

提供對Web應用程式的安全保護，策略管理和監管的持續的集成的解決方案

Cloud Security Framework

Cloud Cloud Security Guidance Document

Cloud Security Products and Services

網路，伺服器和終端

客戶期待安全的雲操作環境

.

維護環境測試和漏洞、入侵管理

- 承租人域之間的隔離
- 信賴的虛擬域：基於策略的安全區域
- 內置的入侵檢測和防護
- 漏洞管理
- 保護機器影響防止損壞和濫用

可用的Cloud產品，服務和解決方案

Cloud Virtual Server Security for VMware

保護雲基礎架構

提供領先的入侵防護，防火牆和虛擬環境安全的可視化管理

Cloud Endpoint Data Protection

敏感資訊的遠程保護

- 阻止丟失或失竊的設備訪問數據
- 敏感數據的存儲，訪問，傳輸或共用保護
- 監控敏感數據的訪問
- 最終用戶級的增強策略管理

Cloud Security Framework

Cloud Cloud Security Guidance Document

Cloud Security Products and Services

物理安全

客戶期望雲數據中心是物理安全的

.

實現一個物理環境的安全計畫

- 確保設備具有適當控制能力以監控訪問
- 防止關鍵領域和設施的未授權訪問.
- 確保所有可直接訪問系統的員工都通過充分的背景檢查。
- 對自然災害可能造成的損失提供足夠的保護

可用的Cloud產品，服務和解決方案

Cloud Physical Security Services

物理環境的安全防護

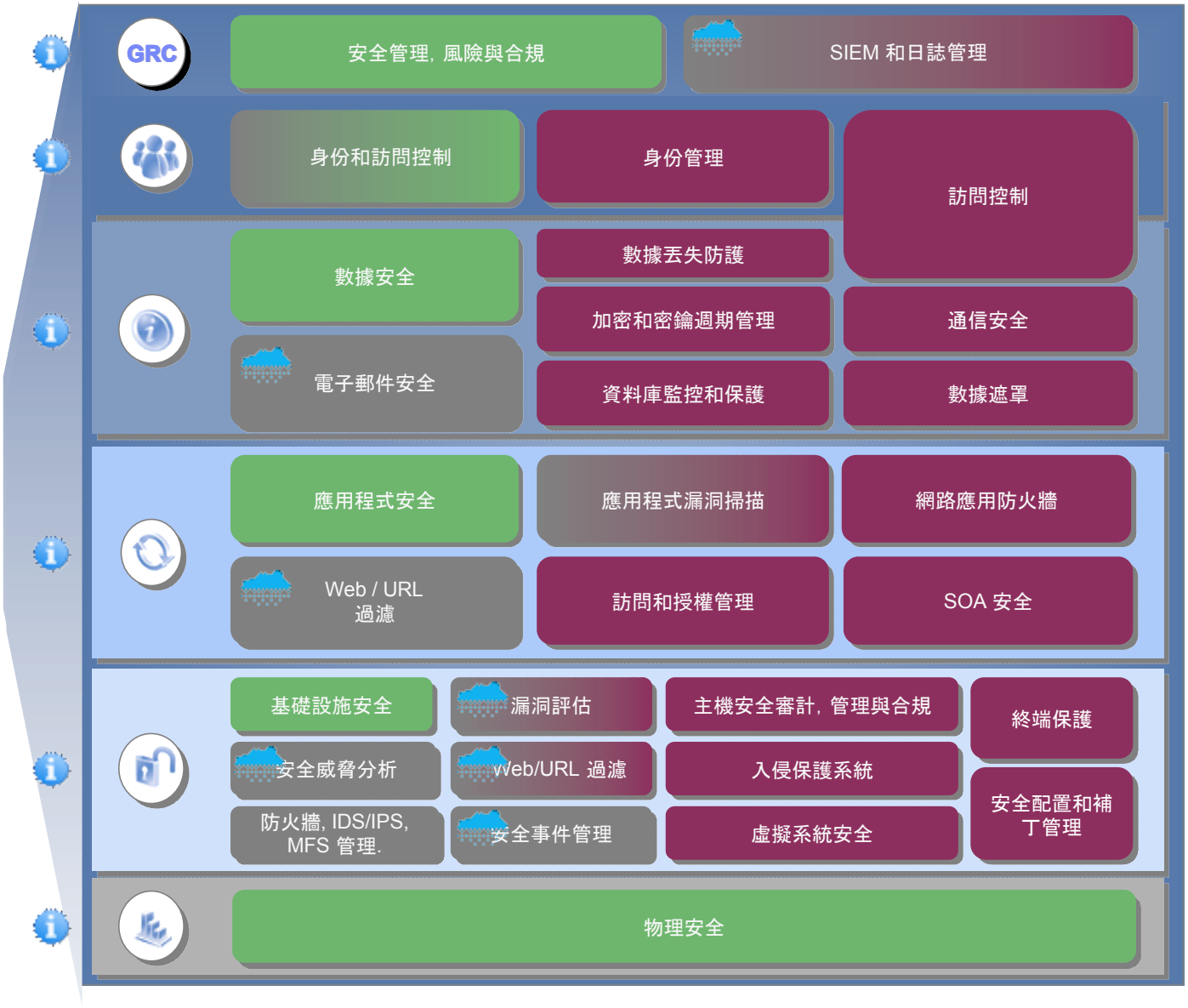
可與您的網路和IT系統集成的整套的數字安全解決方案和現場評估。

Cloud 安全組合 … … 新瓶裝舊酒?

= 專業服務

= 基於雲的服務與管理

= 產品



Smart Security Service Cloud －智慧的安全服務管理雲

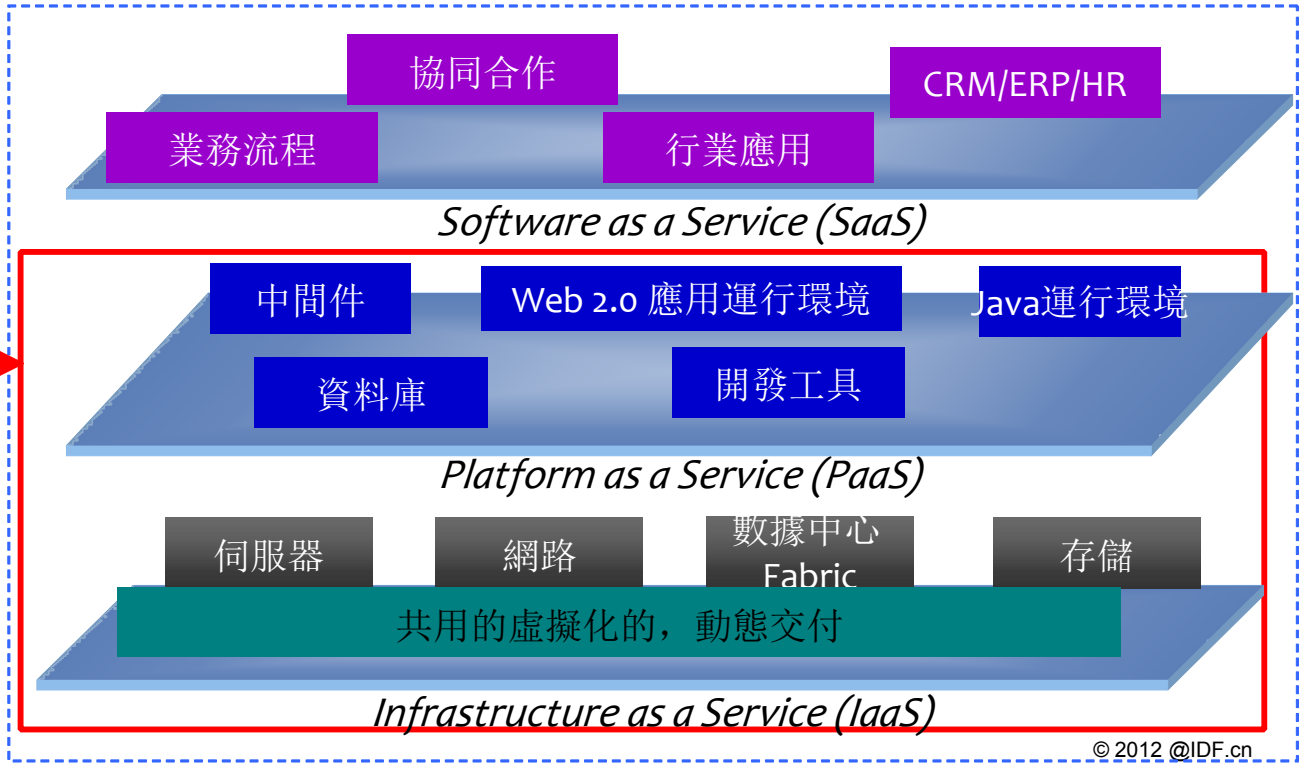
企業級的高性能安全防護軟硬體產品 → 世界級的安全監控系統與取證工具 → 高標準的安全服務管理體系和技術支持回應能力 → *安全服務管理雲*

- ●安全資源共用的服務平臺，全面監控發現與快速回應安全事件
- ●安全管理標準化和自動化，全面提高資訊安全風險管理水準
- ●提高安全事件分析效率，實現安全資源集中和有效分配
- ●快速提高安全事件回應速度,提高安全跨地域管理效率

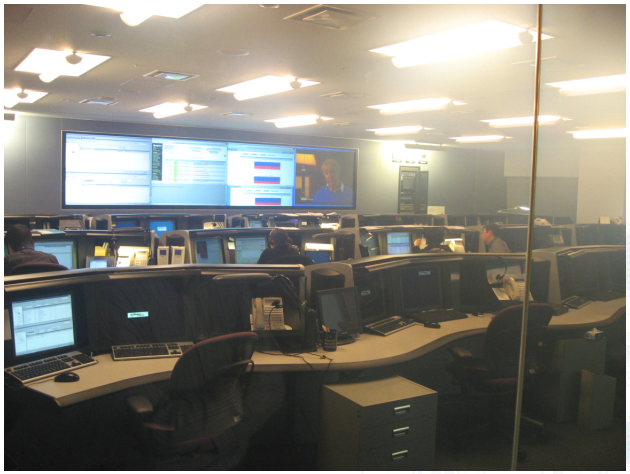
安全服務管理雲

安全服務管理雲

*跨越**PaaS** 層和**IaaS** 層*



Smart Security Service Cloud – 智慧的安全服務管理雲



智慧的安全服務管理雲的架構設計符合資訊安全生命週期PDCA迴圈生態模型和ISO27001等國際資訊安全標準

謝謝!

twitter: @chinawill2012
www.facebook.com/eaglewan
Skype: eaglewan2012