# 駕馭雲端資安破綻，掌握雲端安全攻略

謝侑玲 IBM GTS
CISSP, CISA, CEH

Innovate2013
The IBM Technical Summit
開發者大會

Stay ahead. 先馳得點

# AGENDA

- 雲端趨勢下的安全挑戰
- 企業在雲端環境應俱備的關鍵能力
- IBM 的雲端安全解決方案

# 雲端趨勢下的安全挑戰

# 雲端科技帶來重大的潛在商業及維運效益

虛擬化
- Higher utilization
- Economy-of-scale benefits
- Lower capital expense
- Lower operating expense

標準化
- Easier access
- Flexible pricing
- Reuse and sharing
- Easier integration

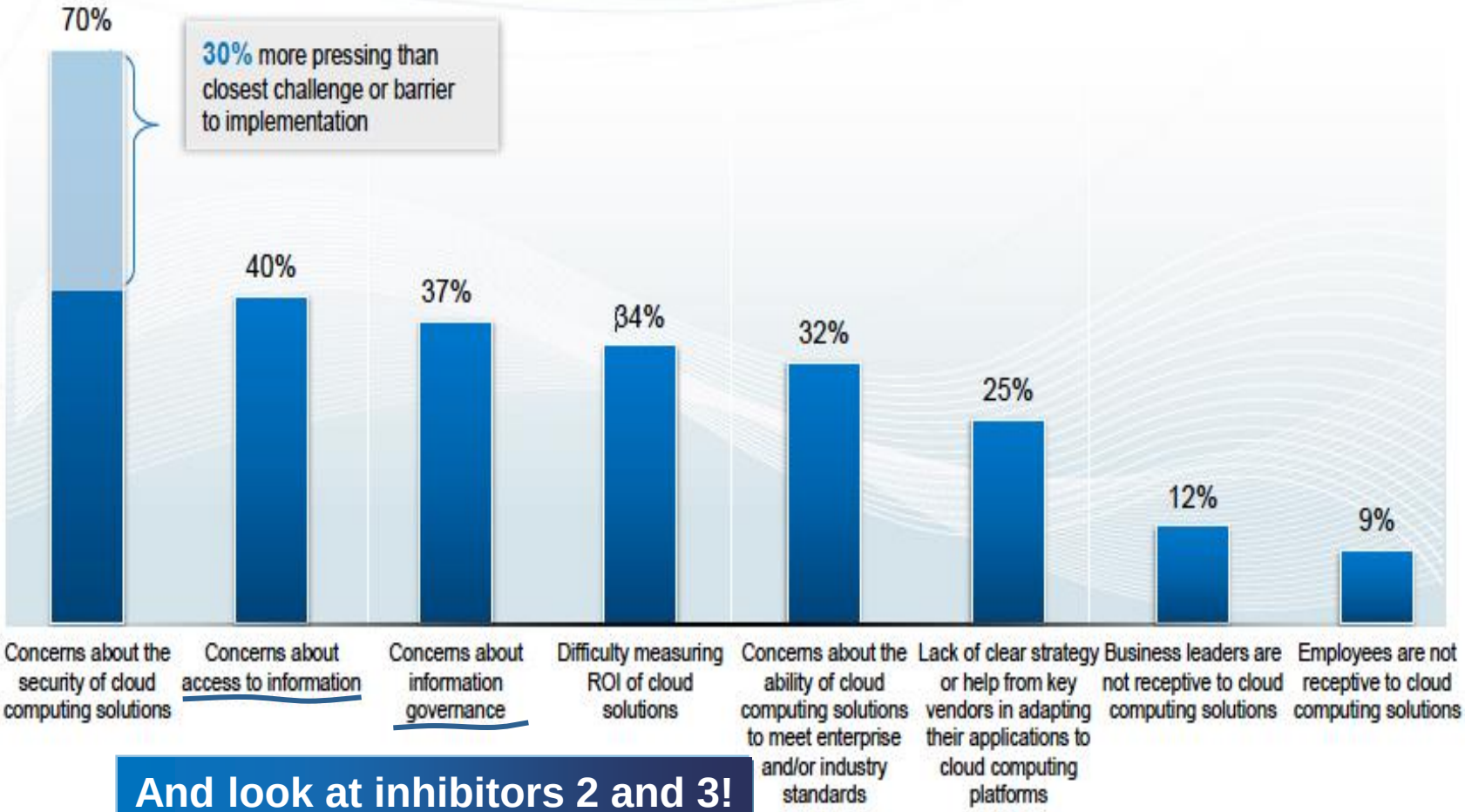
自動化
- Faster cycle times
- Lower support costs
- Optimized utilization
- Better user experience

用較少的資源做更多的事

提供更高的服務彈性

更快速取得所需之資源

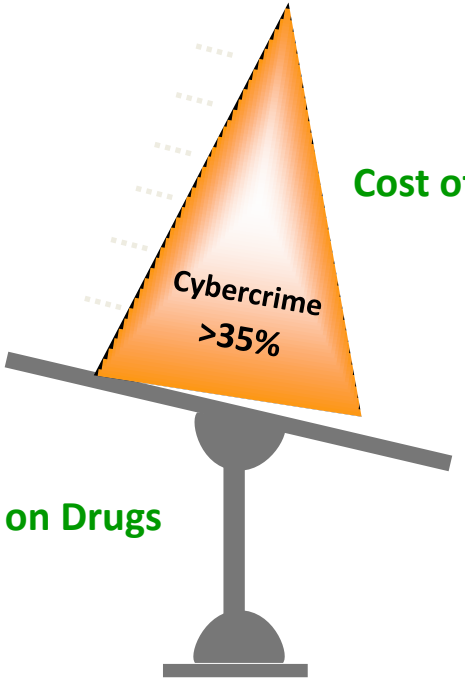
# 但安全顧慮一直是減緩雲端導入的主因之一




**And look at inhibitors 2 and 3!**

*2012 Cloud Computing – Key Trends and Future Effects – IDG*

# 逐漸轉向以竊取敏感資料取得利益的攻擊趨勢
# 更加深多數人對雲端環境的資料安全疑慮




**Cost of Global Cyber Crime**

**$388B**

**Global Black Market on Drugs**

**$288B**

http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02


"You know you can do this just as easily online."

# 雲端環境下的運作模式有別於傳統 IT
# 應該以不同的思維來思考雲端環境的安全


| 現今的資料中心 | 未來的雲端環境 |
| --- | --- |
| 由我們自己控制 | 由誰來控制? |
| ▪設備放在 X 機櫃. | ▪放置在哪裡? |
| ▪資料放在 Y 和 Z 伺服器. | ▪資料存放在何處? |
| ▪我們有備份規劃. | ▪誰為它備份? |
| ▪管理者管制存取權限. | ▪誰具有存取能力? |
| ▪自行規劃系統可用性以符合服務等級. | ▪如何恢復? |
| ▪稽核員可以有效審視. | ▪如何稽核審查? |
| ▪安全團隊參與其中. | ▪安全團隊如何參與? |

# 不同的雲端模式存在不同的安全特性

## 私有雲

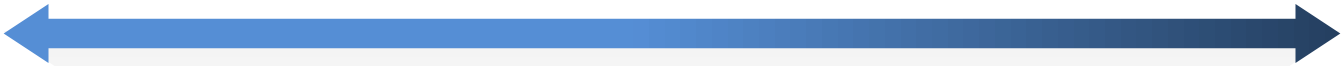
On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party

## 混合 IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability

## 公有雲

Available to the general public or a large industry group and owned by an organization selling cloud services



**對安全和隱私產生的改變**

- 基礎環境為客戶責任
- 較多的安全控制的客製化
- 日常維運過程中有較多的可視性
- 容易取得日誌和政策
- 應用程式和資料在”防火牆”內

- 供應者負擔基礎環境責任
- 較少的安全控制客製化
- 對日常維運過程不具備可視性
- 對日誌和政策難以存取
- 應用程式和資料暴露在外

# 依部署模式或角色不同也會產生不同的安全考慮

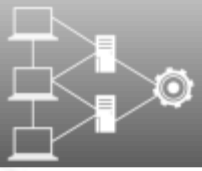
**Infrastructure as a Service (IaaS):** **Cut IT expense and complexity** through cloud data centers

**Platform-as-a-Service (PaaS):** **Accelerate time to market** with cloud platform services

**Innovate business models** by becoming a cloud service provider

**Software as a Service (SaaS):** **Gain immediate access** with business solutions on cloud

| Cloud Enabled Data Center | Cloud Platform Services | Cloud Service Provider | Business Solutions on Cloud |
|---|---|---|---|
| 主要安全考量：<br>基礎架構和身份管理 | 主要安全考量：<br>應用程式和資料 | 主要安全考量：<br>基礎架構資料和合規 | 主要安全考量：<br>合規和治理 |
| ▪ Manage datacenter identities<br>▪ Secure virtual machines<br>▪ Patch default images<br>▪ Monitor logs on all resources<br>▪ Network isolation | ▪ Secure shared databases<br>▪ Encrypt private information<br>▪ Build secure applications<br>▪ Keep an audit trail<br>▪ Integrate existing security | ▪ Isolate cloud tenants<br>▪ Policy and regulations<br>▪ Manage security operations<br>▪ Build compliant data centers<br>▪ Offer backup and resiliency | ▪ Harden exposed applications<br>▪ Securely federate identity<br>▪ Deploy access controls<br>▪ Encrypt communications<br>▪ Manage application policies |



# 雲端環境下的關鍵安全能力

# IBM Security Framework 提供 IBM 內部及客戶一個結構化的框架以思考資訊安全議題

Built to meet four key requirements:

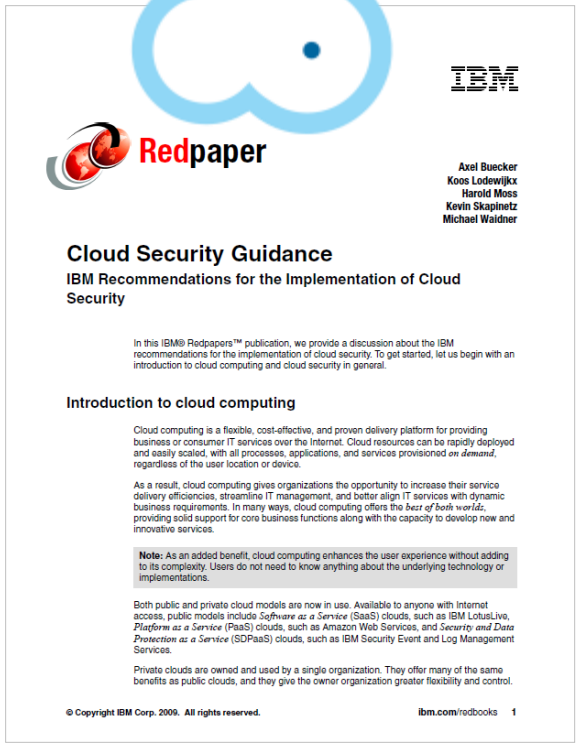
- Provide *Assurance*
- Enable *Intelligence*
- Automate *Process*
- Improve *Resilience*


*Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;*

*IBM RedGuide REDP-4528-00, July 2009*

# IBM 雲端安全指引

- Based on cross-IBM research and customer interaction on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:
  - *Building a Security Program*
  - *Confidential Data Protection*
  - *Implementing Strong Access and Identity*
  - *Application Provisioning and De-provisioning*
  - *Governance Audit Management*
  - *Vulnerability Management*
  - *Testing and Validation*



IBM

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

**Cloud Security Guidance**

**IBM Recommendations for the Implementation of Cloud Security**

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

**Introduction to cloud computing**

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

**Note:** As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.



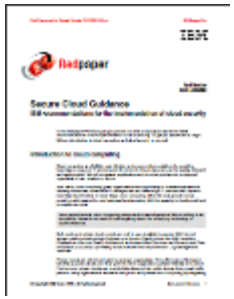




12

# Security Intelligence, Governance and Compliance


IBM Security Framework




IBM Cloud Security Guidance Document

Need **Insight** to the security posture and **Compliance** to the regulations of the cloud.

## Implement a governance and audit management program

- Establish third-party audits (SAS 70, ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Insight into change, incident, image management, etc.
- Support for forensics and e-Discovery
- Provide visibility into virtual Infrastructure
- Maintain audit logs for compliance and audit readiness

## Additional Security Capabilities for the cloud

- **Evaluating existing security policies, processes, postures for the cloud environment to create a roadmap to reduced risk**
- **Extend the auditing/logging capabilities to the virtualized infrastructure**

# 建立涵蓋雲端架構環境的安全稽核記錄和事件分析

Accesses end-to-end audit reports for the customer application

Joe – Security & Compliance Manager
(Cloud Service Provider)

Requests resources for running regulated workload (composite App) on the cloud

Susan – Cloud Service Requestor

Generates reports for audit and compliance, and detects security offenses

Security Proxy (IBM Security Identity and Access Manager)

Cloud Service Consumers

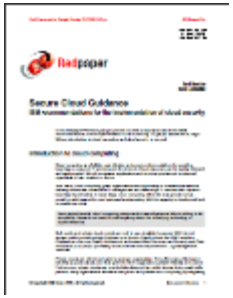
SSO

Cloud Environments


Radar SIEM

Application, middleware administration and system logs and events


IBM Security Framework




IBM Cloud Security Guidance Document

## People and Identity

Need **proper authentication** of cloud users.

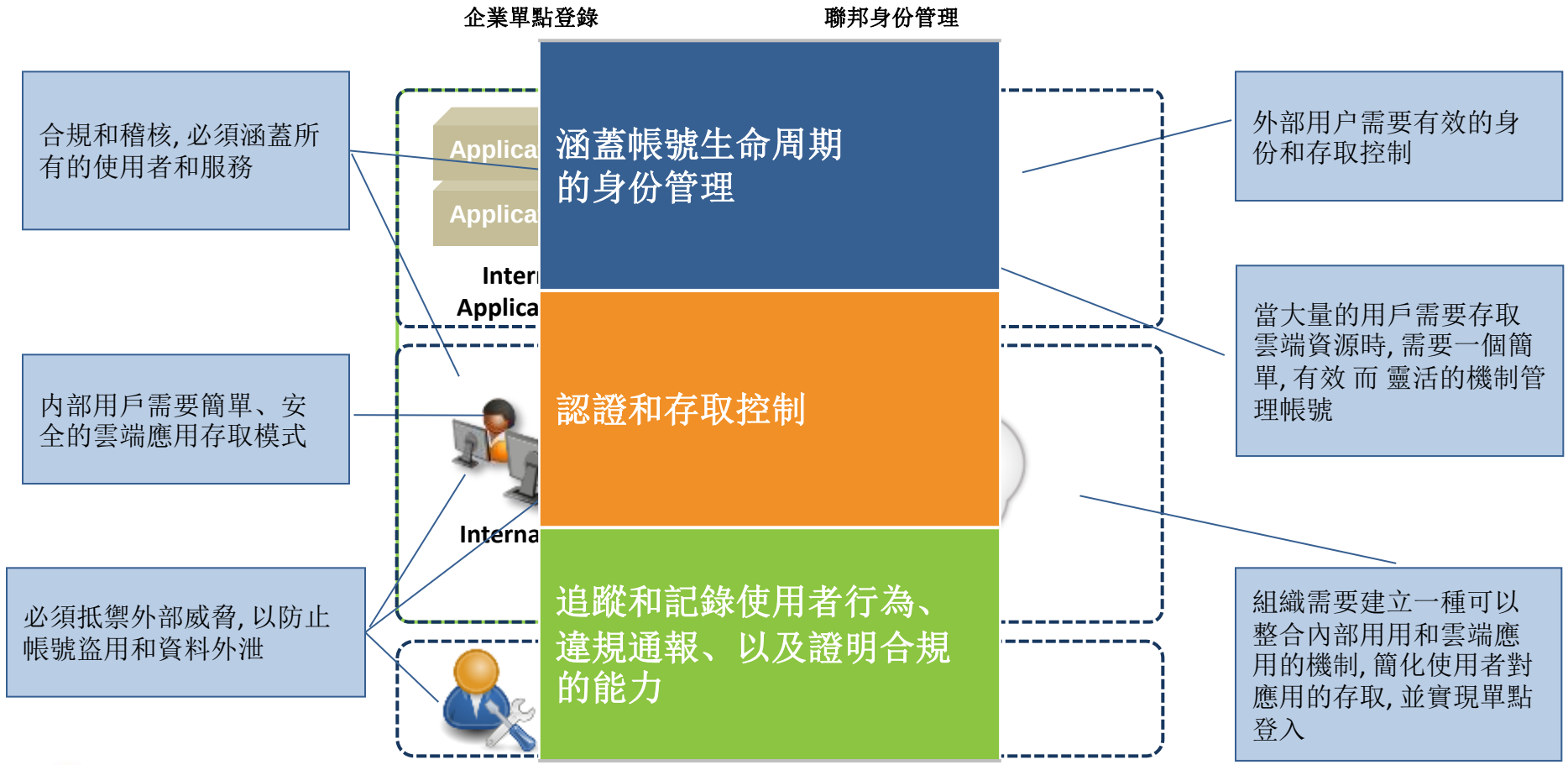
### Implement strong identity and access management

- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third-party systems
- A standards-based, single-sign-on capability can help simplify user logons for both internally hosted applications and the cloud.
- Role Based Access Control (RBAC) reduces the risk associated with persons being assigned inappropriate access and retaining access .

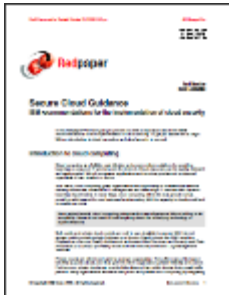
### Additional Security Capabilities for the cloud

- **Extend the identity management process to cloud environment**
- **Securely manage cloud identities and user access to cloud applications**

# 建立標準化且有效的雲端用戶註冊和存取管理




IBM Security Framework




IBM Cloud Security Guidance Document

# Data and Information

**Data protection** is the **most important** concern on the cloud.

## Ensure confidential data protection

- Develop data classification standard and policy to set up the data usage, storage and destroy guideline on the cloud
- Use a secure network protocol when connecting to a secure information store.
- Implement a isolation mechanism for the virtualization environment
- Setup Data Lost Protection and data usage monitoring mechanism for confidential information

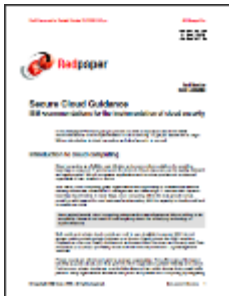
## Additional Security Capabilities for the cloud

- **Develop/Extend the data protection policy to include the cloud environment**
- **Strength the Virtualization environment protection**

# 強化雲端資料安全的四個參考步驟

| | | |
|---|---|---|
| 1 | **Understand, define policy** | ▪ Discover where sensitive data resides<br>▪ Classify and define data types<br>▪ Define policies and metrics |
| 2 | **Secure and protect** | ▪ Encrypt, redact and mask virtualized databases<br>▪ De-identify confidential data in non-production environments |
| 3 | **Actively monitor and audit** | ▪ Monitor virtualized databases and enforce review of policy exceptions<br>▪ Automate and centralize the controls needed for auditing and compliance (e.g., SOX, PCI)<br>▪ Assess database vulnerabilities |
| 4 | **Establish compliance and security intelligence** | ▪ Automate reporting customized for different regulations to demonstrate compliance in the Cloud<br>▪ Integrate data activity monitoring with security information and event management (SIEM) |


IBM Security Framework




IBM Cloud Security Guidance Document

# Application

## Need a **secure cloud applications** and **provider processes**.

### Establish application and environment provisioning

- Implement a program for application and image provisioning.
- A secure application testing program should be implemented.
- Ensure all changes to virtual images and applications are logged.
- Develop all web-based applications using secure coding guidelines.

### Additional Security Capabilities for the cloud

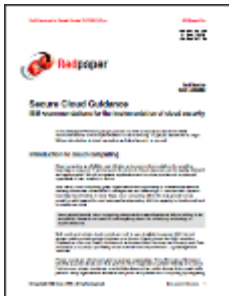
- **Develop the application lifecycle management and ensure a secure application deployments**


IBM Security Framework

# Infrastructure

## Customers expect a **secure** cloud **operating environment**.

### Maintain environment testing and vulnerability/intrusion management




IBM Cloud Security Guidance Document

- Isolation between tenant domains
- Trusted virtual domains: policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability and patch management
- Protect machine images from corruption and abuse

### Additional Security Capabilities for the cloud

- **Develop Hypervisor level security policy and image management**
- **Develop the hypervisor level intrusion prevention, firewall and security for virtual environments**
- **Extend the auditing and patch management to hypervisor level**

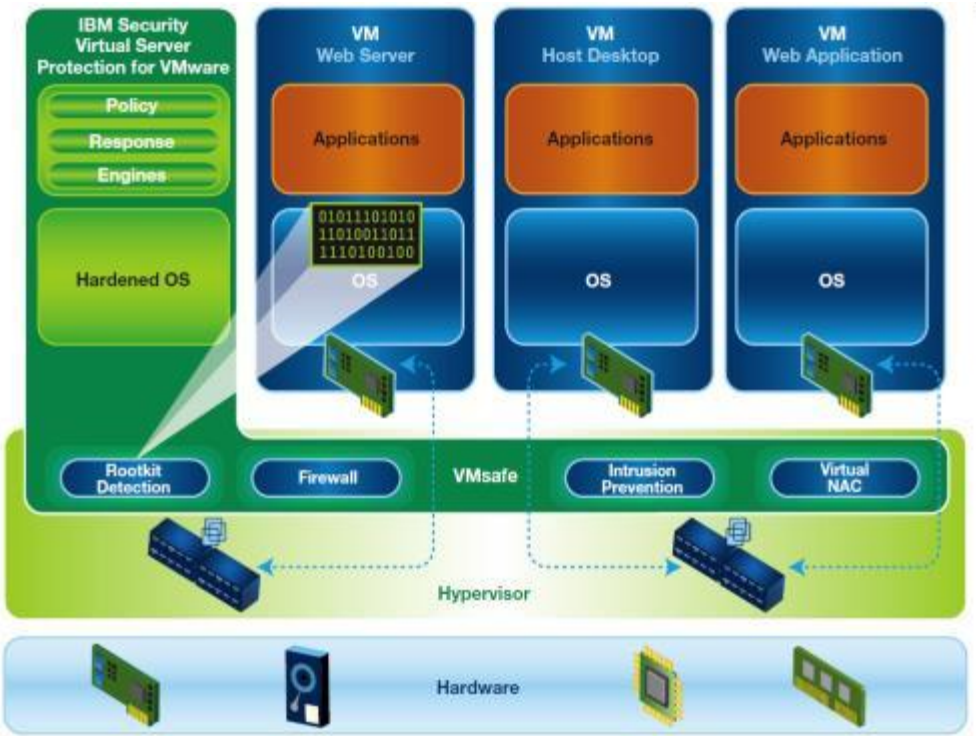
# 虛擬化帶來全新的複雜性及保護模式

## 虛擬化帶來新的複雜性

- VM 可能會被動態遷移
- 增加新的架構層級需要管理及保護
- 多個系統或應用共存不易進行實體區隔
- Hypervisor 成為新攻擊點, VM 攻擊溢出可能影響其他 VM

## 虛擬環境下之保護模式

- 建立 VM 保護及 Image 管理
- 提升管理帳戶之管理
- 建立虛擬層的網路區隔及安全保護(入侵防禦, 防火牆)
- 透過 API 降低個別系統分別安裝 Agent 之負載



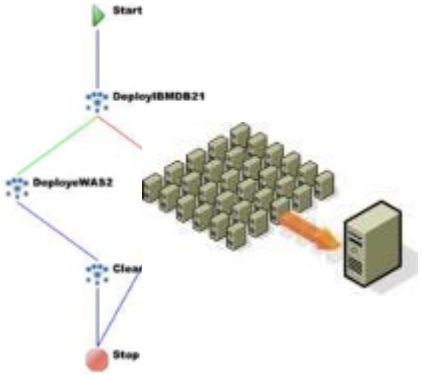
# 跨實體與虛擬環境的修正程式和安全設定管理

終端設備

+


實體伺服器

+




虛擬伺服器

**主要考慮:**

- 針對終端設備, 實體伺服器, 虛擬伺服器, 雲端資源分別管理修正程式需要多重管理機制及大量時間
- 多數虛擬伺服器的修正方式和安全參數檢查通常不足

**應俱備之能力**

- 建立管理不同平台(不同作業系統, 跨終端設備平台, 應用程式, 雲端資產) 的整合修正管理方案
- 縮短修正程式派送時間及增加達成率
- 俱備隊執行中 /離線 /修眠中的 VM 的修正管理
- 持續的監控和安全配置管理

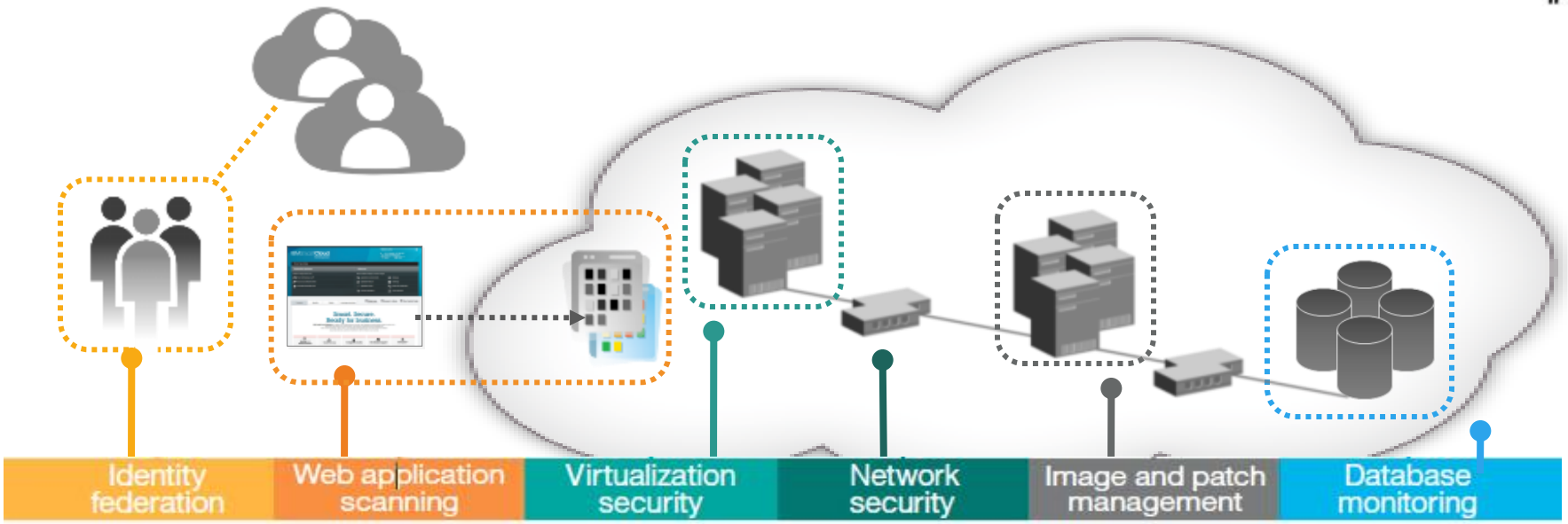
# IBM 的雲端安全建議方案

# IBM 從兩個面向提供客戶雲端安全

| Security for the Cloud | Security from the Cloud |
| --- | --- |
| *Helping clients begin their journey to the cloud with relevant security expertise* | *Cloud-based Security Services that help reduce costs and complexity, improve sec. posture, and meet regulatory compliance* |

These services solve client skill gaps, assess for weaknesses, assist with strategy development /execution, and protect against threats.

# IBM 在雲端環境的各個環節都提供完整的解決方案




| Federating identities for public and hybrid clouds | Application Scanning for cloud based applications | VM protection for VMware hosts and workloads | Virtual IPS for virtual network edge protection | Automated patch management for virtual endpoints | Database activity monitoring and protection |
|---|---|---|---|---|---|
| **Federated Identity Manager – Business Gateway** | **AppScan Static / Dynamic Analysis** | **Virtual Server Protection for VMware** | **Network IPS Virtual Appliance** | **Tivoli Endpoint Manager - SmartCloud Patch** | **Guardium database monitoring and protection** |

Security Intelligence and Analytics — **QRadar Security Intelligence Platform**

SC MAGAZINE AWARDS 2012 WINNER Honored in the U.S. — IBM won Best Cloud Security Solutions Company

Exa CORPORATION — Creating a secure hybrid private cloud with FIM / VSP

FIBERLINK® — Built a cloud-based, endpoint management service with TEM

# 並針對客戶建立安全的雲端環境需求提供對應服務

Professional Service


Understand how to leverage cloud capabilities while considering business needs and governance requirements

Professional Service


Helps cloud providers (public / private / hybrid) assess the security of a cloud against best practices and mandates.

Managed Service

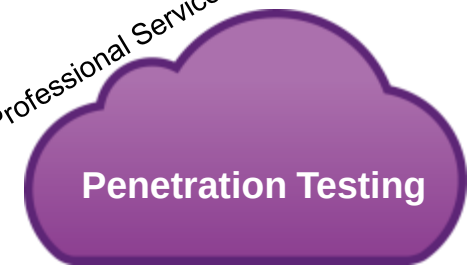

Helps provide protection from a broad selection of threats by actively mitigating cloud attacks

**Consultative services**

**Assess or secure the cloud**

**For cloud providers or enterprises**

Professional Service




Validates the security of components of the cloud through active exploitation and system penetration

Professional Service

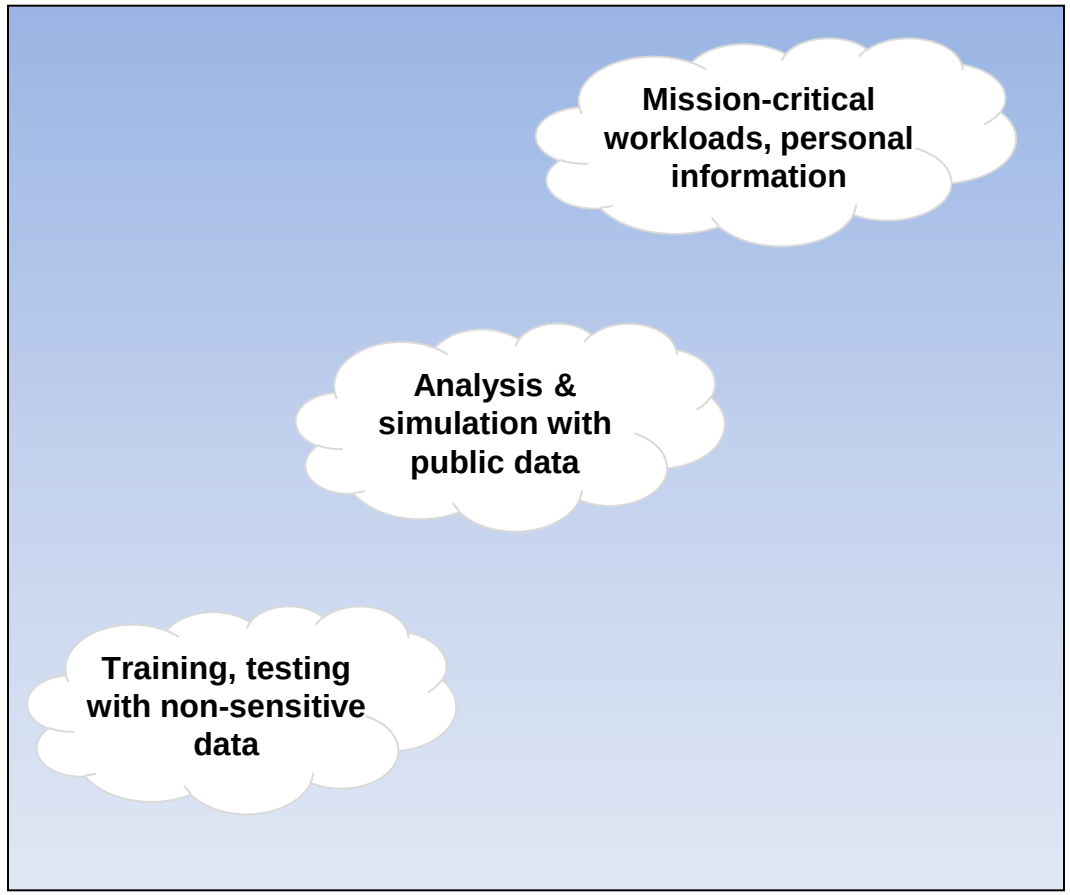

Assesses the authentication strategy of a cloud environment and provides a plan for optimizing the approach against established business goals

Professional Service


Assesses web-based cloud applications via automated scanning and manual source code review

# 並在世界各地提供雲端模式的安全服務模式

# 雲端環境依其工作負載不同會有不同的風險及安全管理需求, 難以透過單一的方案解決所有問題




**Tomorrow's high value / high risk workloads need:**

- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

**Today's clouds are primarily here:**

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

# IBM 的雲端安全導入模式根據客戶的不同階段需求及負載特性提供適合的方案

## Design

Establish a cloud strategy and implementation plan to get there.

## Deploy

Build cloud services, in the enterprise and/or as a cloud services provider.

## Consume

Manage and optimize consumption of cloud services.

| | | | |
|---|---|---|---|
| **IBM Cloud Security Approach** | ***Secure by Design*** *Focus on building security into the fabric of the cloud.* | ***Workload Driven*** *Secure cloud resources with innovative features and products.* | ***Service Enabled*** *Govern the cloud through ongoing security operations and workflow.* |
| **Example security capabilities** | ▪ Cloud security roadmap<br>▪ Secure development<br>▪ Network threat protection<br>▪ Server security<br>▪ Database security | ▪ Application security<br>▪ Virtualization security<br>▪ Endpoint protection<br>▪ Configuration and patch management | ▪ Identity and access management<br>▪ Secure cloud communications<br>▪ Managed security services |

# 透過 IBM 的諮詢服務可以取得一個安全轉型到雲端應用環境的導入策略藍圖

## Define a cloud strategy with security in mind

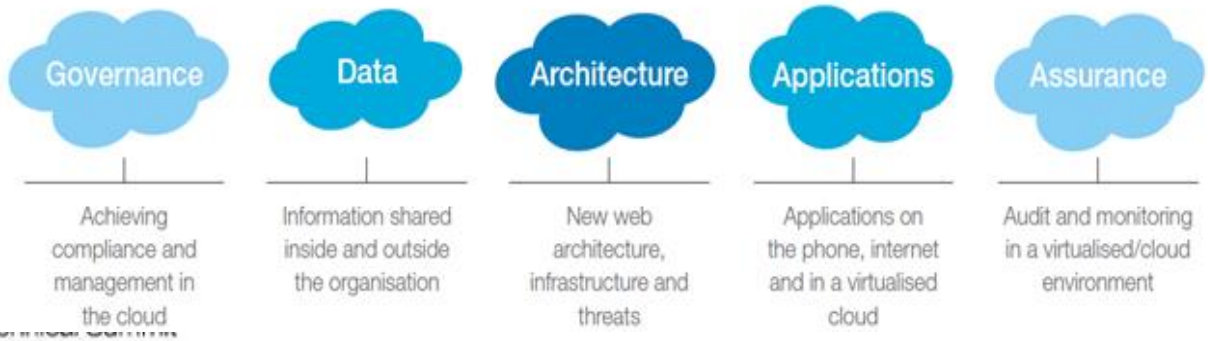
- Identify the different workloads and how they need to interact.
- Which models are appropriate based on their security and trust requirements and the systems they need to interface to?

## Identify the security measures needed

- Using a framework such as the one IBM uses, the IBM Security Framework and Blueprint, allows teams to capture the measures that are needed in areas such as governance, architecture, applications and assurance.

## Enabling security for the cloud

- Define the upfront set of assurance measures that must be taken.
- Assess that the applications, infrastructure and other elements meet the security requirements, as well as operational security measures.



# IBM 的安全產品在業界居於領導地位

| Domain | Segment / Report | Analyst Recognition |
|---|---|---|
| Security Intelligence, Analytics and GRC | Security Information & Event Management (SIEM) | 2012, 2010 |
| | Enterprise Governance Risk & Compliance Platforms | 2011, 2011 |
| People | Identity & Access Governance | 2012 |
| | User Provisioning / Administration | 2012 |
| | Role Management & Access Recertification | 2011, 2012*** |
| | Enterprise Single Sign-on (ESSO) | 2011*, 2010 |
| | Web Access Management (WAM) | 2012** |
| Data | Database Auditing & Real-Time Protection | 2011 |
| | Data Masking | 2013 |
| Applications | Static Application Security Testing (SAST) | 2010, 2010 |
| | Dynamic Application Security Testing (DAST) | 2011 |
| Infrastructure | Network Intrusion Prevention Systems (NIPS) | 2012, 2010 |
| | EndPoint Protection Platforms (EPP) | 2013 |

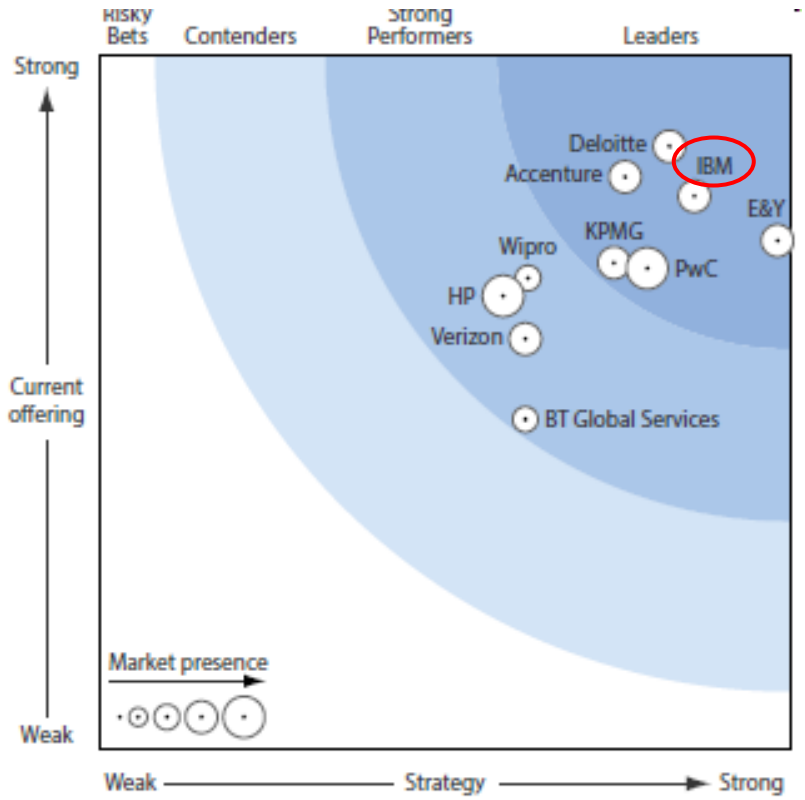
* Gartner MarketScope (discontinued in 2012)
** Gartner MarketScope
*** 2012 IDC MarketScape ranked IBM #1 in IAM

Gartner: Leader | Visionary | Niche Player | Challenger
FORRESTER: Leader | Strong Performer | Contender
IDC: Leader (#1, 2, or 3 in segment)

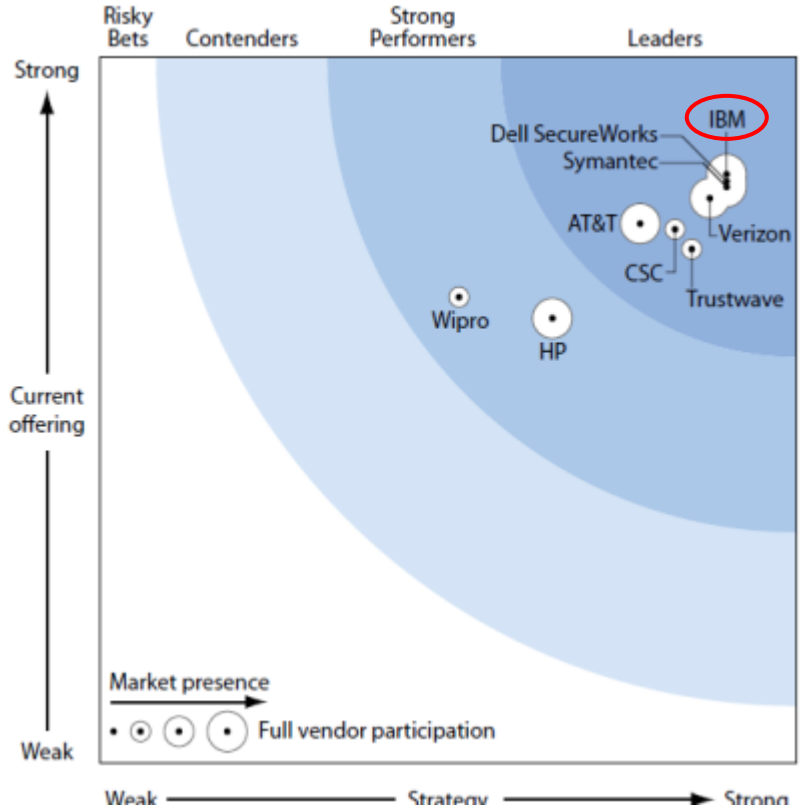
V13-05

# 在顧問服務以及雲端管理服務也居於領先地位

*Security Consulting*




*Managed Security Services*




Source: Forrester Research Inc. “Forrester Wave™”: Information Security Consulting Services, Q1 2013”. And Forester Wave: Managed Security Services providers Q1, 2012

Full report can be accessed at http://www.ibm.com

ibm.com/security