麟瑞科技
RING LINE CORPORATION

雲端世代的 資訊安全防護

張晃崚 CCIE #13673

麟瑞科技 區域銷售事業處

什麼是雲端運算？

看看這些人怎麼說........

"It's stupidity. It's worse than stupidity: it's a marketing hype campaign”

-Richard Stallman,
founder of the Free Software Foundation

"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane.”

-Larry Ellison, Oracle CEO

NIST 所定義的雲端運算

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Google 翻譯

- 雲計算是一種模式使方便，按需網絡訪問共享池配置的計算資源（如網絡，服務器，存儲，應用程序和服務），可以迅速配置和發布以最小的管理工作或服務提供商相互作用

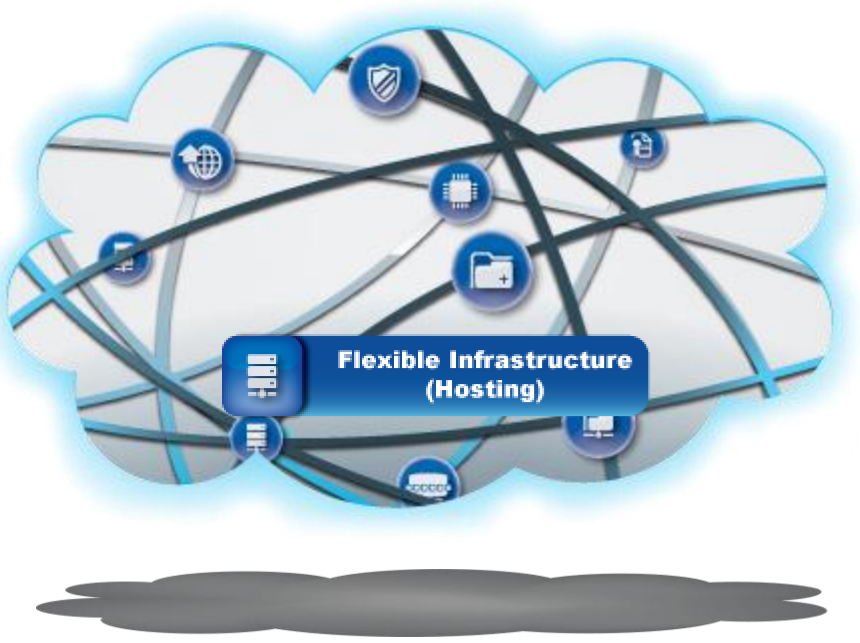
Source: National Institute of Standards and Technology, Version 15, 10-7-09

雲端運算的本質之一
Infrastructure as a Services

Flexible Infrastructure
(Hosting)

彈性的運用實體資料中心的資源

- 系統及網路管理人員可以隨使用單位的需求, 機動的提供 ICT 架構
- 每個部門都可以擁有自己的虛擬資料中心, 可自行或委託管理.
- 資源可重覆使用, 機動調派, 提昇整體利用率, 達成綠色節能的目地.
- 案例如 : Rackspace 及 Amazon AWS EC2.

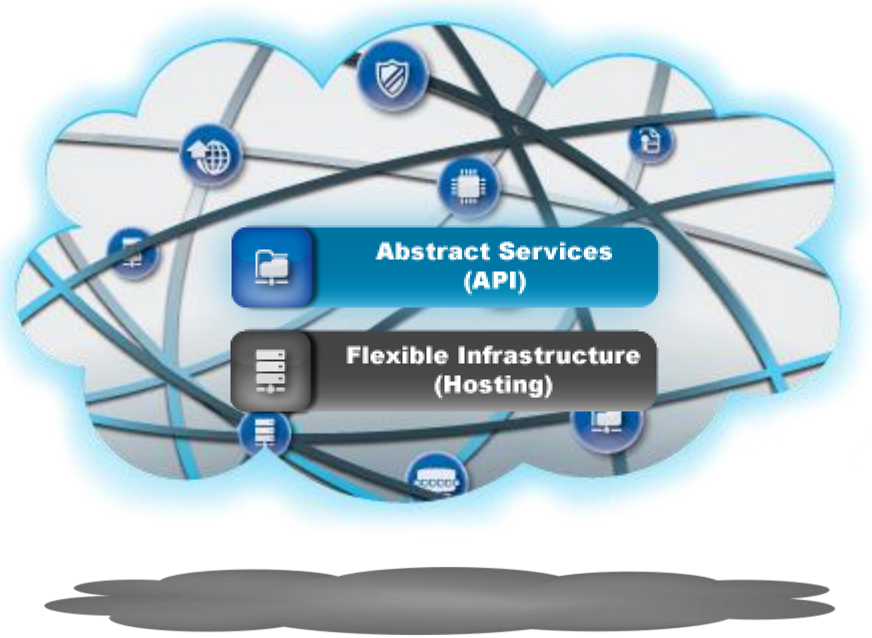


雲端運算的本質之二
Platform as a Services

Abstract Services (API)

以應用程式設計為導向的平台服務.

- 程式設計人員可以依據所提供的 API, 自行開發所需要的程式系統, 而不需要知道這個平台在那裡.
- 資源可重覆使用, 負載均衡, 網路安全, 資料備援等皆可自動達成.
- 案例如 : Google Application Engine, Amazon AWS Simple Storage 及 Cisco WebEx Connect 等.



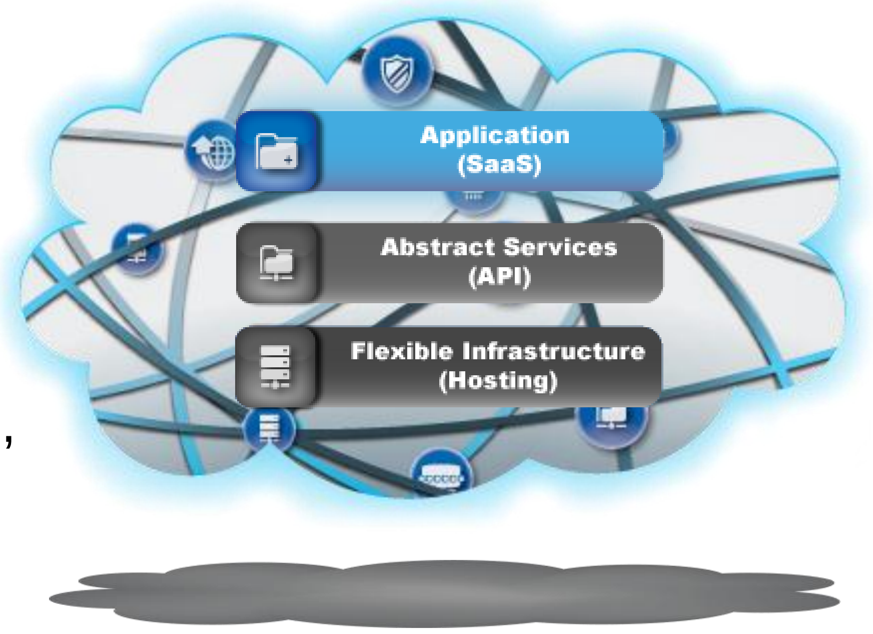
雲端運算的本質之三

Software as a Services

Application
(SaaS)

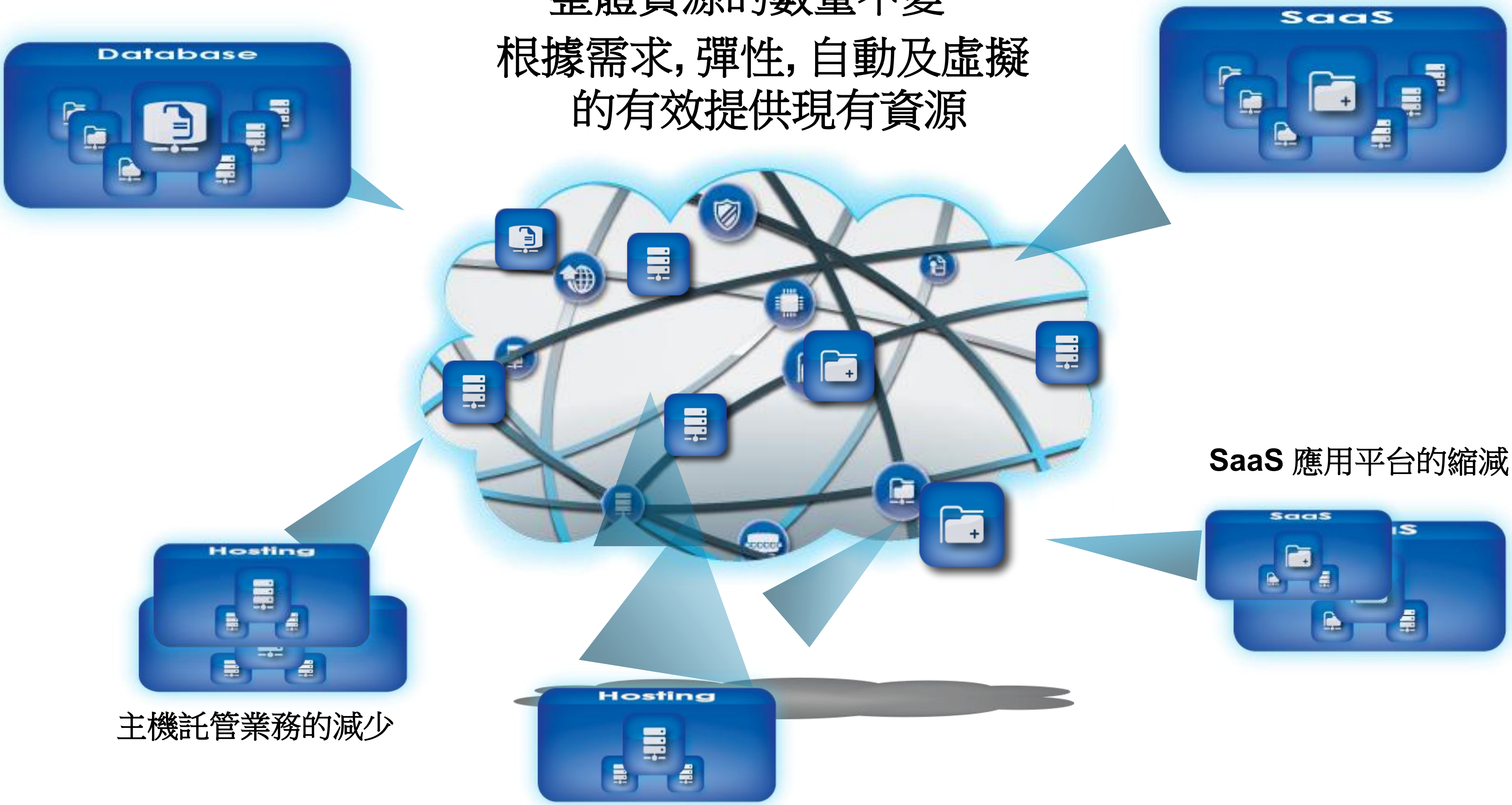
以應用為導向的服務.

- 一般使用者可依據需求直接使用各項服務系統, 而不需要知道該系統存放在那裡.
- 使用者可以直接利用瀏覽器來使用應用程式服務.
- 以 dotcom 的形式存在.
- 案例如 : Gmail, Cisco WebEx.com, Salesforce.com and qq.com 等.



雲端運算的需求

機動的增減資源的使用與自動化



資料庫叢集的增生

整體資源的數量不變

根據需求, 彈性, 自動及虛擬的有效提供現有資源

SaaS 應用平台的增生

SaaS 應用平台的縮減

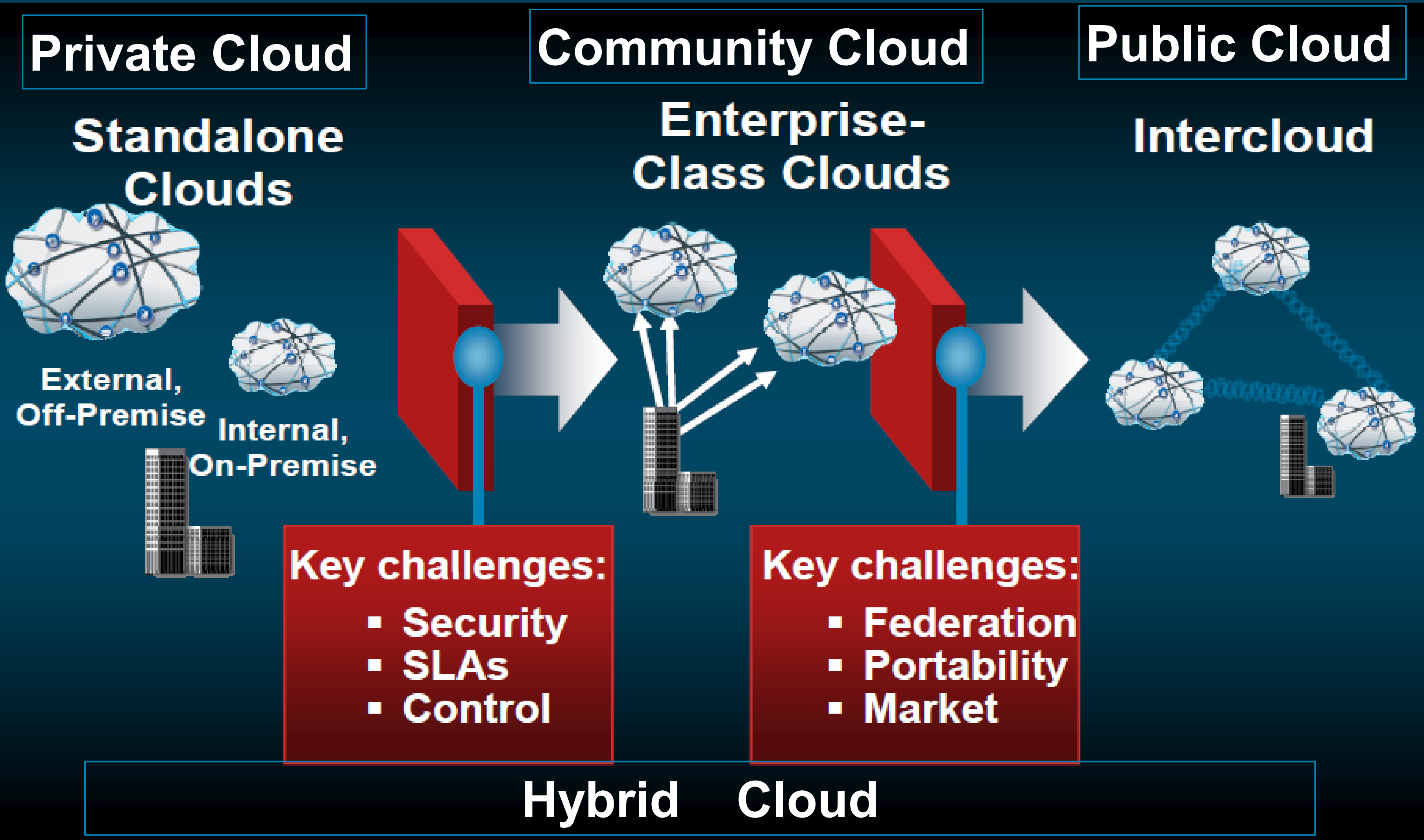
主機託管業務的減少

虛擬化主機業務的增加

Common Cloud Characteristics

- Cloud computing often leverages:
    - Massive scale
    - Homogeneity
    - Virtualization
    - Resilient computing
    - Low cost software
    - Geographic distribution
    - Service orientation
    - Advanced security technologies

雲端運算在技術上的挑戰



Private Cloud

Standalone Clouds

External, Off-Premise

Internal, On-Premise

Community Cloud

Enterprise-Class Clouds

Public Cloud

Intercloud

Key challenges:

- Security
- SLAs
- Control

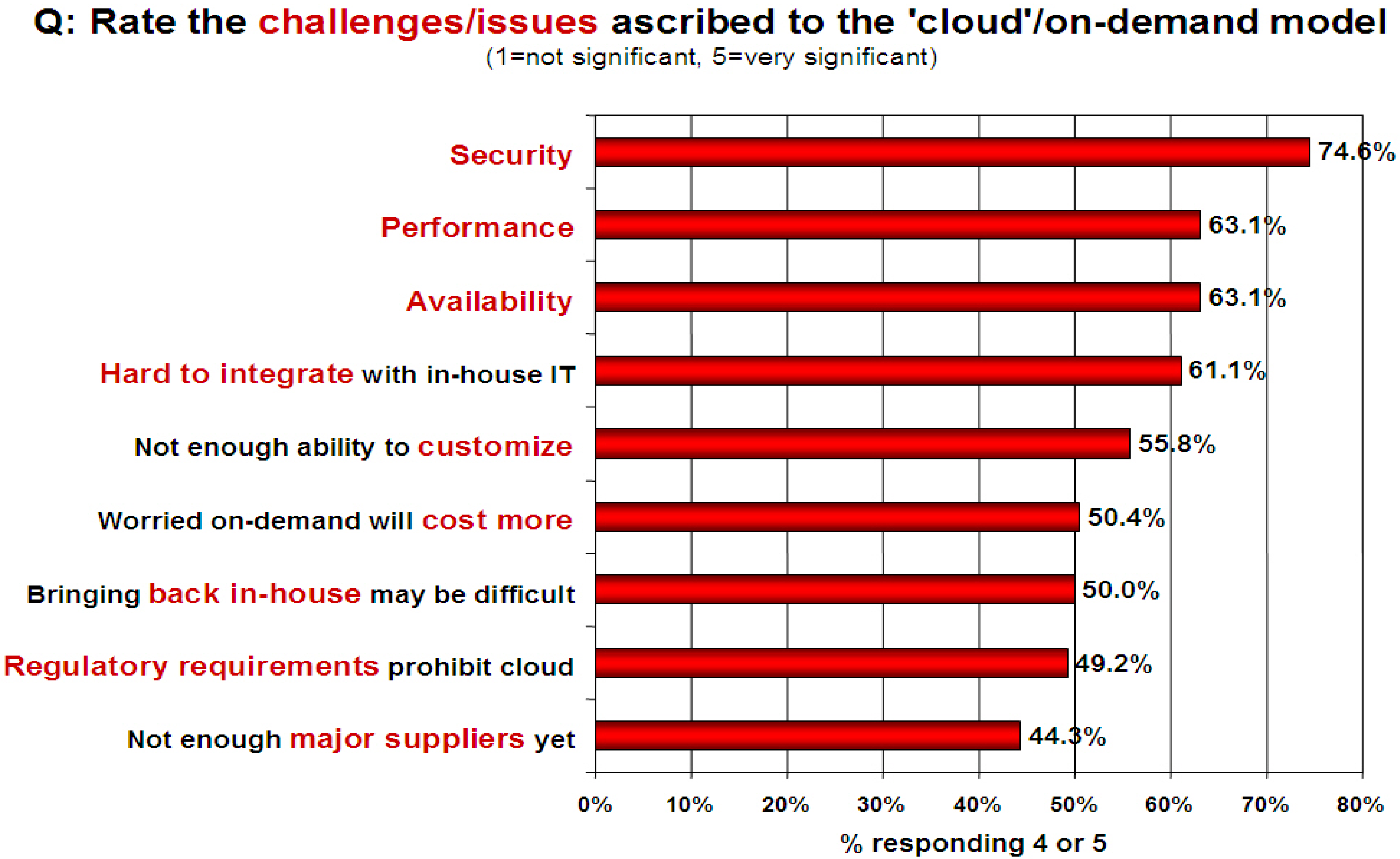
Key challenges:

- Federation
- Portability
- Market

Hybrid Cloud

Cloud Computing Security

Security is the Major Issue



Source: IDC Enterprise Panel, August 2008 n=244

Analyzing Cloud Security

- Some key issues:
    - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
    - There are both advantages and challenges

Former Intel CEO, Andy Grove: “only the paranoid survive”

General Security Advantages

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

General Security Challenges

- Trusting vendor’s security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can’t be examined
- Loss of physical control

Security Relevant Cloud Components

- Cloud Provisioning Services
- Cloud Data Storage Services
- Cloud Processing Infrastructure
- Cloud Support Services
- Cloud Network and Perimeter Security
- Elastic Elements: Storage, Processing, and Virtual Networks

Provisioning Service

- Advantages
  - Rapid reconstitution of services
  - Enables availability
    - Provision in multiple data centers / multiple instances
  - Advanced honey net capabilities
- Challenges
  - Impact of compromising the provisioning service

Data Storage Services

- Advantages
  - Data fragmentation and dispersal
  - Automated replication
  - Provision of data zones (e.g., by country)
  - Encryption at rest and in transit
  - Automated data retention
- Challenges
  - Isolation management / data multi-tenancy
  - Storage controller
    - Single point of failure / compromise?
  - Exposure of data to foreign governments

Cloud Processing Infrastructure

- Advantages
  - Ability to secure masters and push out secure images
- Challenges
  - Application multi-tenancy
  - Reliance on hypervisors
  - Process isolation / Application sandboxes

Cloud Support Services

- Advantages
    - On demand security controls (e.g., authentication, logging, firewalls…)
- Challenges
    - Additional risk when integrated with customer applications
    - Needs certification and accreditation as a separate application
    - Code updates

Cloud Network and Perimeter Security

- Advantages
  - Distributed denial of service protection
  - VLAN capabilities
  - Perimeter security (IDS, firewall, authentication)
- Challenges
  - Virtual zoning with application mobility

Cloud Security Advantages Part 1

- Data Fragmentation and Dispersal
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Fault Tolerance and Reliability
- Greater Resiliency
- Hypervisor Protection Against Network Attacks
- Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)

Cloud Security Advantages Part 2

- Simplification of Compliance Analysis
- Data Held by Unbiased Party (cloud vendor assertion)
- Low-Cost Disaster Recovery and Data Storage Solutions
- On-Demand Security Controls
- Real-Time Detection of System Tampering
- Rapid Re-Constitution of Services
- Advanced Honeynet Capabilities

Cloud Security Challenges Part 1

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees

Cloud Security Challenges Part 2

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest

Additional Issues

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
  - FISMA
  - HIPAA
  - SOX

Secure Migration Paths for Cloud Computing

The ‘Why’ and ‘How’ of Cloud Migration

- There are many benefits that explain **why** to migrate to clouds
    - Cost savings, power savings, green savings, increased agility in software deployment
- Cloud security issues may drive and define **how** we adopt and deploy cloud computing solutions

Balancing Threat Exposure and Cost Effectiveness

- Private clouds may have less **threat exposure** than community clouds which have less threat exposure than public clouds.
- Massive public clouds may be more **cost effective** than large community clouds which may be more cost effective than small private clouds.
- *Doesn't strong security controls mean that I can adopt the most cost effective approach?*

Cloud Migration and Cloud Security Architectures

- Clouds typically have a single security architecture but have many customers with different demands
    - Clouds should attempt to provide configurable security mechanisms
- Organizations have more control over the security architecture of private clouds followed by community and then public
    - This doesn’t say anything about actual security
- Higher sensitivity data is likely to be processed on clouds where organizations have control over the security model

Putting it Together

- Most clouds will require very strong security controls
- All models of cloud may be used for differing tradeoffs between threat exposure and efficiency
- There is no one “cloud”. There are many models and architectures.
- How does one choose?

Migration Paths for Cloud Adoption

- Use public clouds
- Develop private clouds
  - Build a private cloud
  - Procure an outsourced private cloud
  - Migrate data centers to be private clouds (fully virtualized)
- Build or procure community clouds
  - Organization wide SaaS
  - PaaS and IaaS
  - Disaster recovery for private clouds
- Use hybrid-cloud technology

Possible Effects of Cloud Computing

- Small enterprises use public SaaS and public clouds and minimize growth of data centers
- Large enterprise data centers may evolve to act as private clouds
- Large enterprises may use hybrid cloud infrastructure software to leverage both internal and public clouds
- Public clouds may adopt standards in order to run workloads from competing hybrid cloud infrastructures

麟瑞科技

RING LINE CORPORATION