Cloud Security Issues and Adoption Guideline for Thai Government Agencies

July 26, 2016

Dr. Sudsanguan Ngamsuriyaroj
sudsanguan.nga@mahidol.ac.th

Faculty of ICT, Mahidol University

Agenda

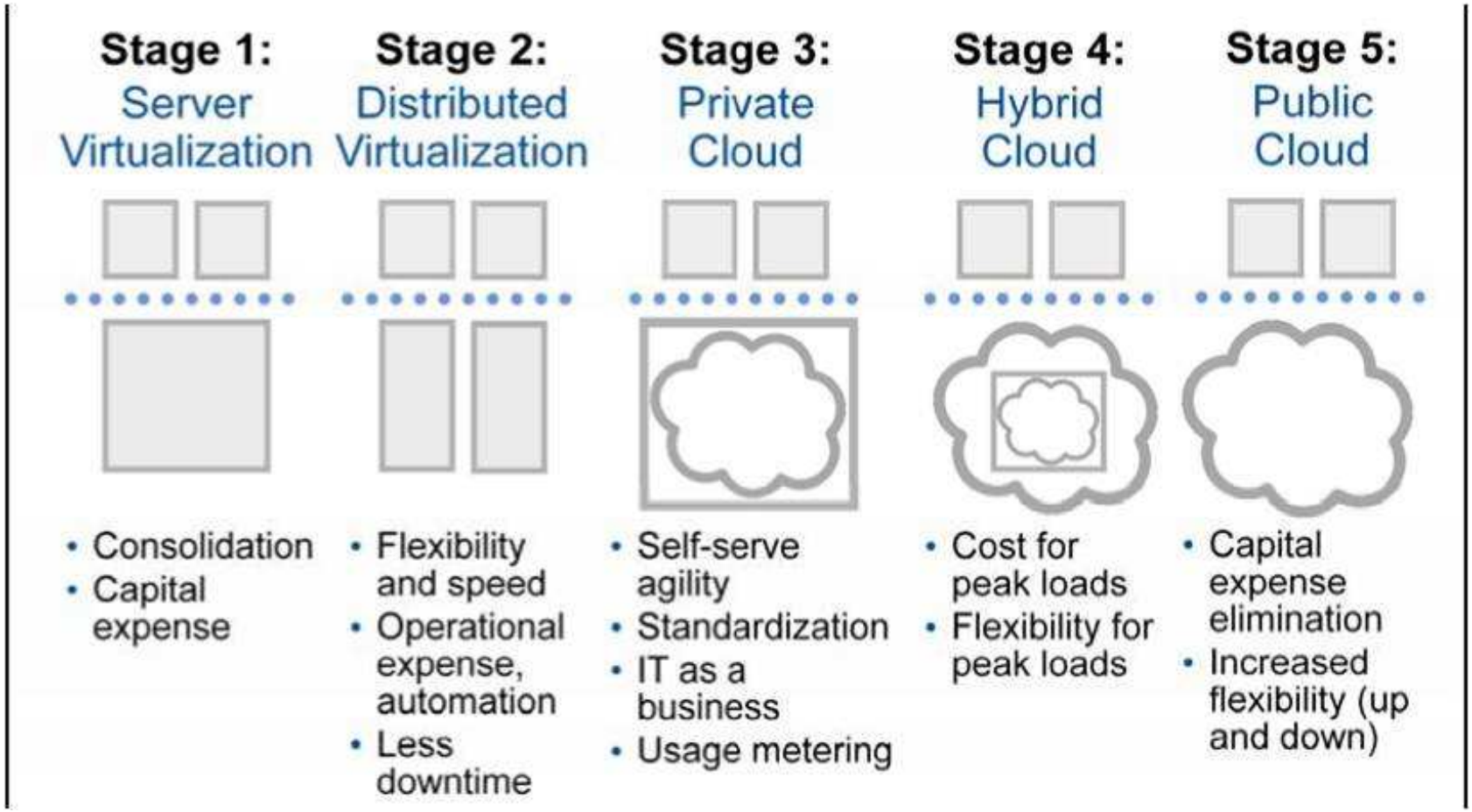
Cloud Adoption Guideline

General Security Concepts

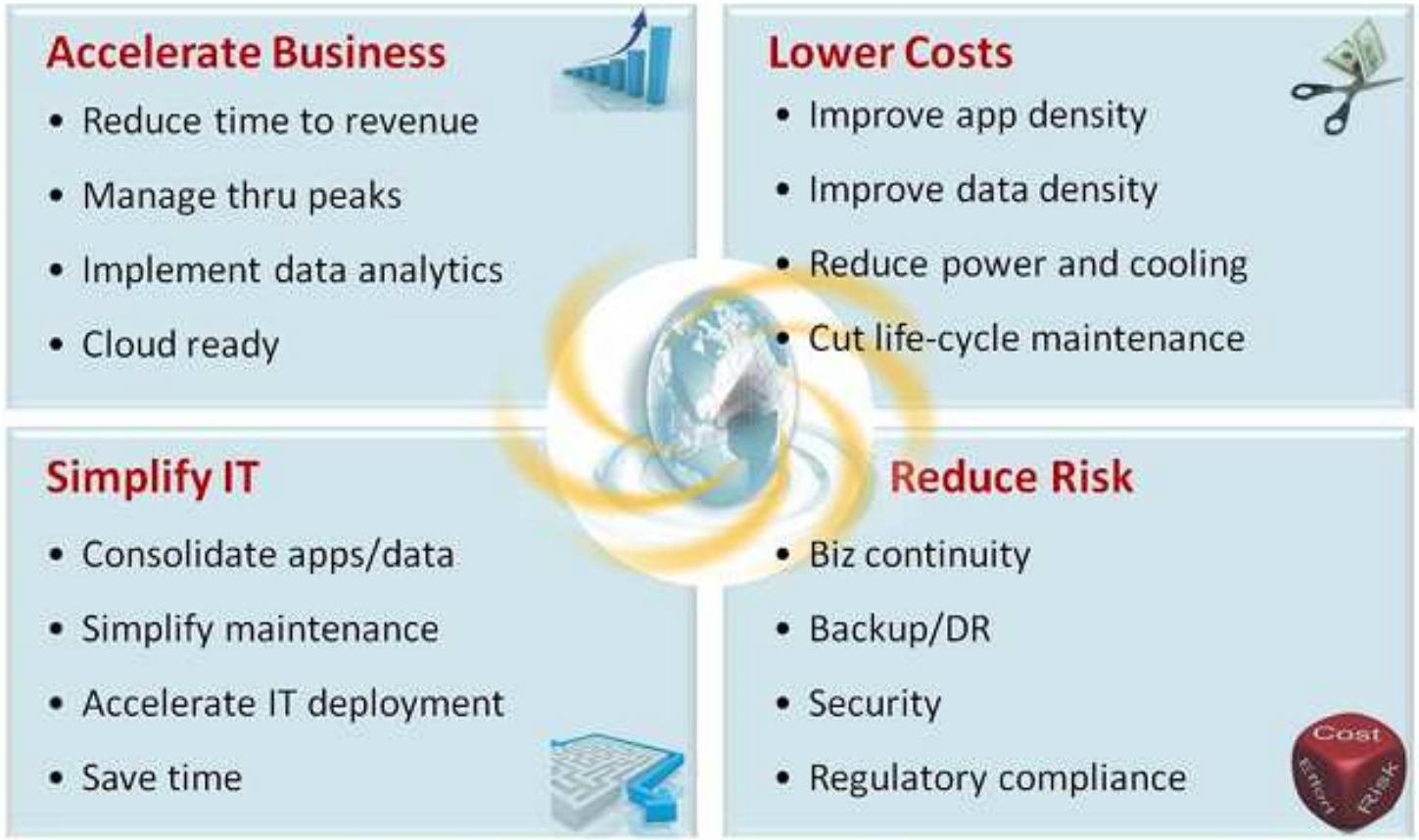
Cloud Security Model

Cloud Security Issues

Cloud Adoption from Data Center to Cloud

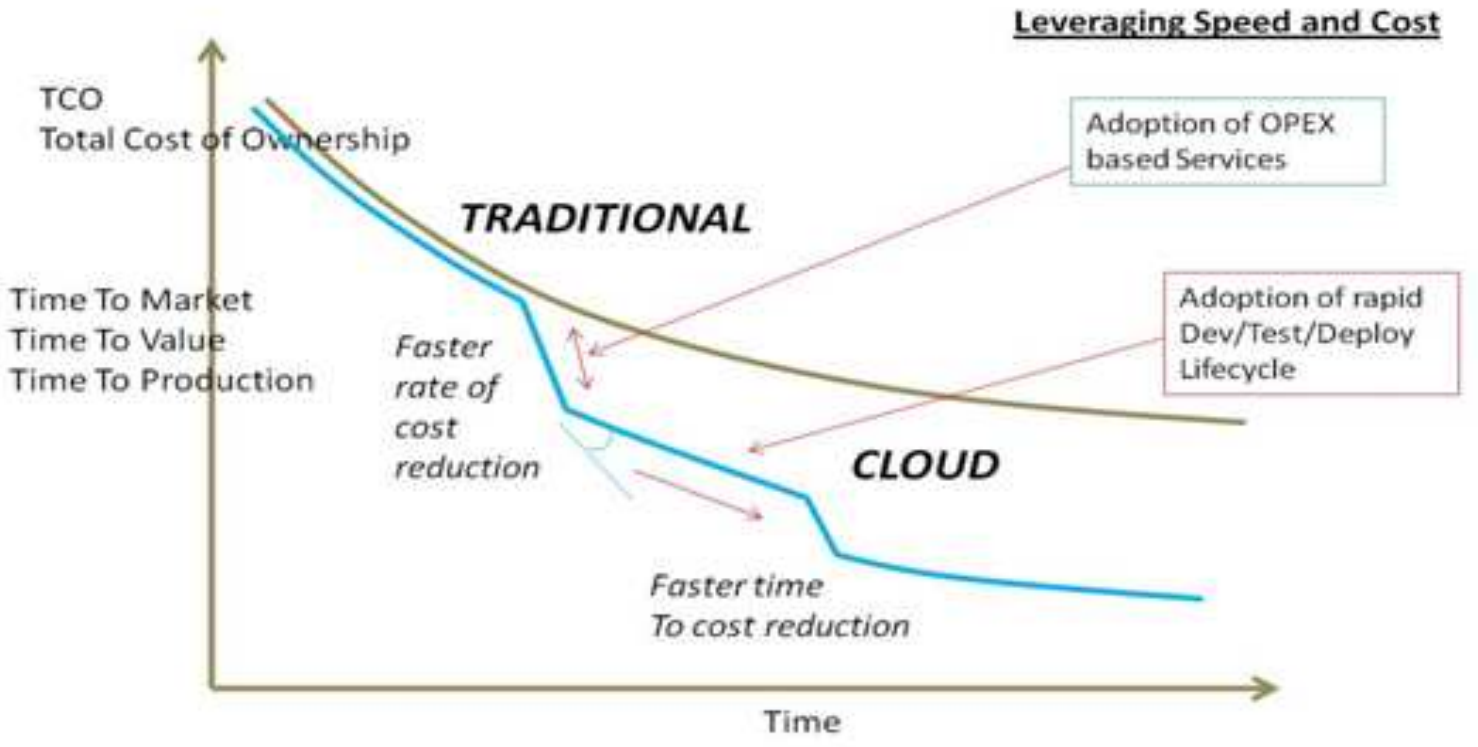


Cloud Adoption – Why?



Source: IDC, 2014

Cloud Adoption – Why?
Cost Reduction



Are you ready for Cloud?

Which applications will be moved to cloud

Readiness of existing infrastructure

Development of IT personnel (infrastructure and developers)

How to migrate to cloud

- Which cloud model/platform (public, private, hybrid) to use

Budget / ROI

Application users

Schedule to deliver products/services

Which applications will be moved to Cloud

Categories of Applications

1. Public applications: for everyone: web sites
2. External based applications: for customers/ partners
3. Internal based applications: for staff only - emails
4. Private applications: for administration: ERP, HR

Readiness of Existing Infrastructure

- Network infrastructure
- System infrastructure
- Application platforms
- BCP – Business Continuity Plan
- Infrastructure Maintenance
- Audit process

Readiness of Existing Infrastructure: Network Ready?

- Physical / Logical network diagram (latest update?)
- All existing equipment and their capacity
- Report of network usage
  - Bandwidth enough?
  - Any usage abuse?
- What links needed to be updated

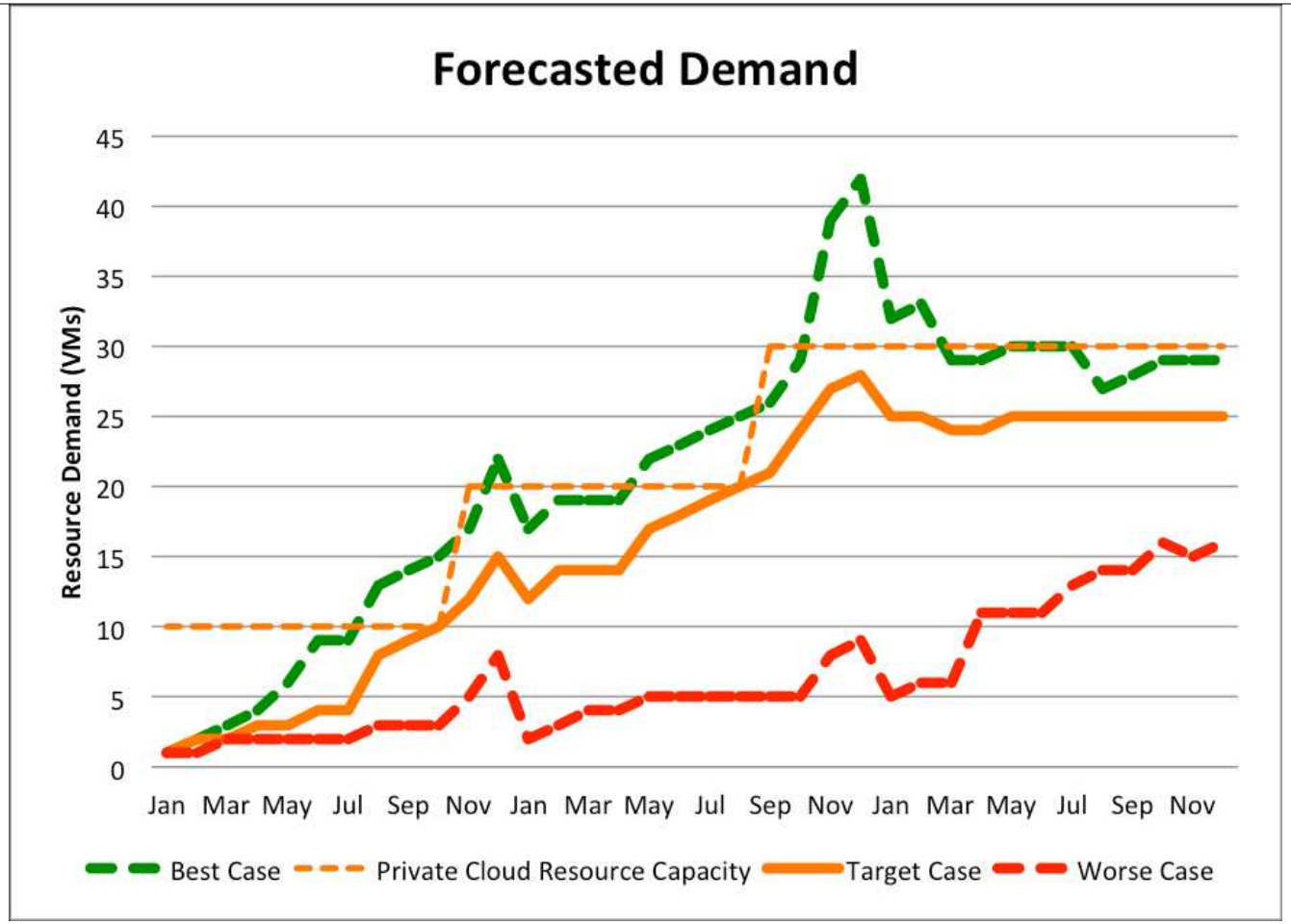
Readiness of Existing Infrastructure: System Ready?

- List of all servers and the applications running

	ชื่อเครื่อง /รุ่น	ปี	การใช้งาน	RAM	Disk	Storage

- List of all servers no longer used
- How long a server will be used
- Is there any maintenance?
- What workload running and how much the utilization is?
- If there is a new server, a plan to use VM ?

Workload Forecasted



Workload Analysis

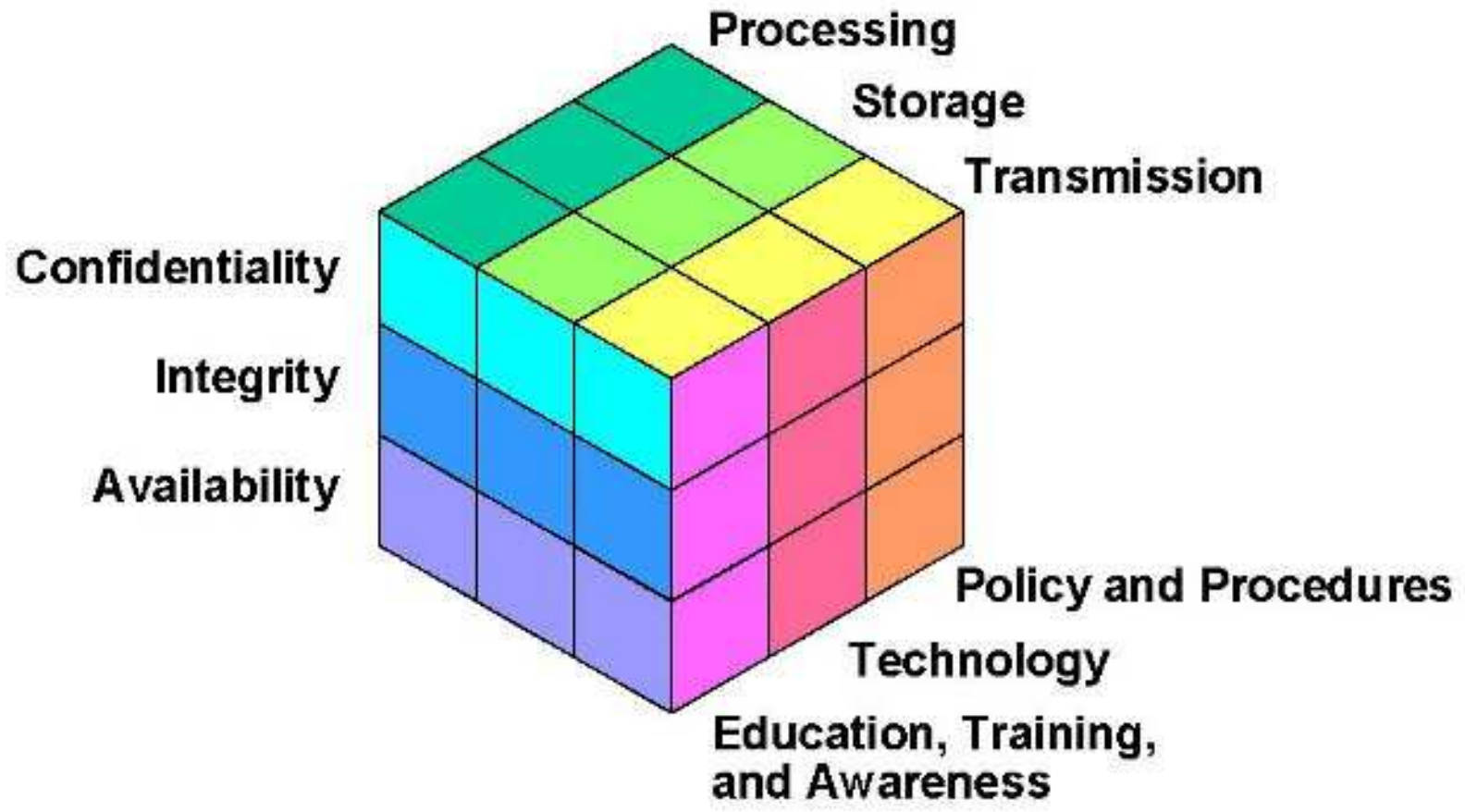
	Web	Application	Database	Other
Production	5	20	2	
BI	2	2 (20 VMs)	1	
Other		12 (30 VMs)		
Dev/Test	2	2	1	7
Performance Testing (QA)	3	10	2	
Total	12	46 (+50 VMs)	6	7

Realm	Element	Number of Instances	Storage Size (per instance)	Type	12-month Growth
Dev	Web Server	2	120 GB	Local	0%
Dev	App Server	2	120 GB	Local	0%
Dev	*OrderNow* Database	1	20 GB	Local	0%
Dev	VSS (operating software)	2	120 GB	Local	0%
Dev	VSS (source files, etc)	Shared	50 GB	SAN	25%
Dev	General (ad hoc)	3	250 GB	Local	0%
QA	Web Server	5	250 GB	Local	10%
QA	App Server	10	120 GB	Local	10%
QA	Oracle Engine	2	120 GB	Local	0%
QA	*OrderNow* Database	Shared	500 GB	SAN	15%

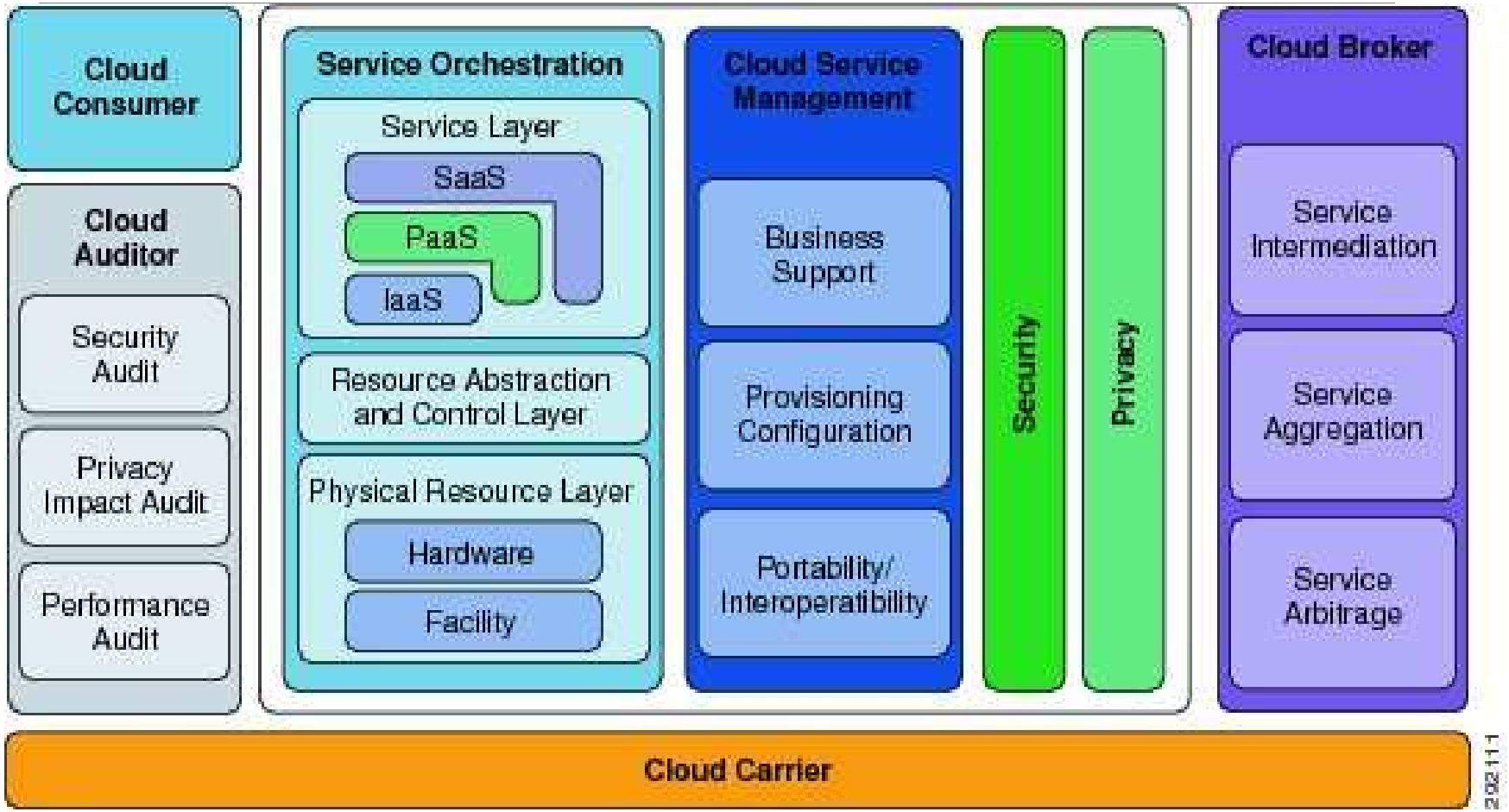
What would be Barriers?

- Data security and privacy
- People with effective skills
- Different cloud service providers and platforms
- Vendor lock-in
- Cloud providers' reliability and availability
- Risks

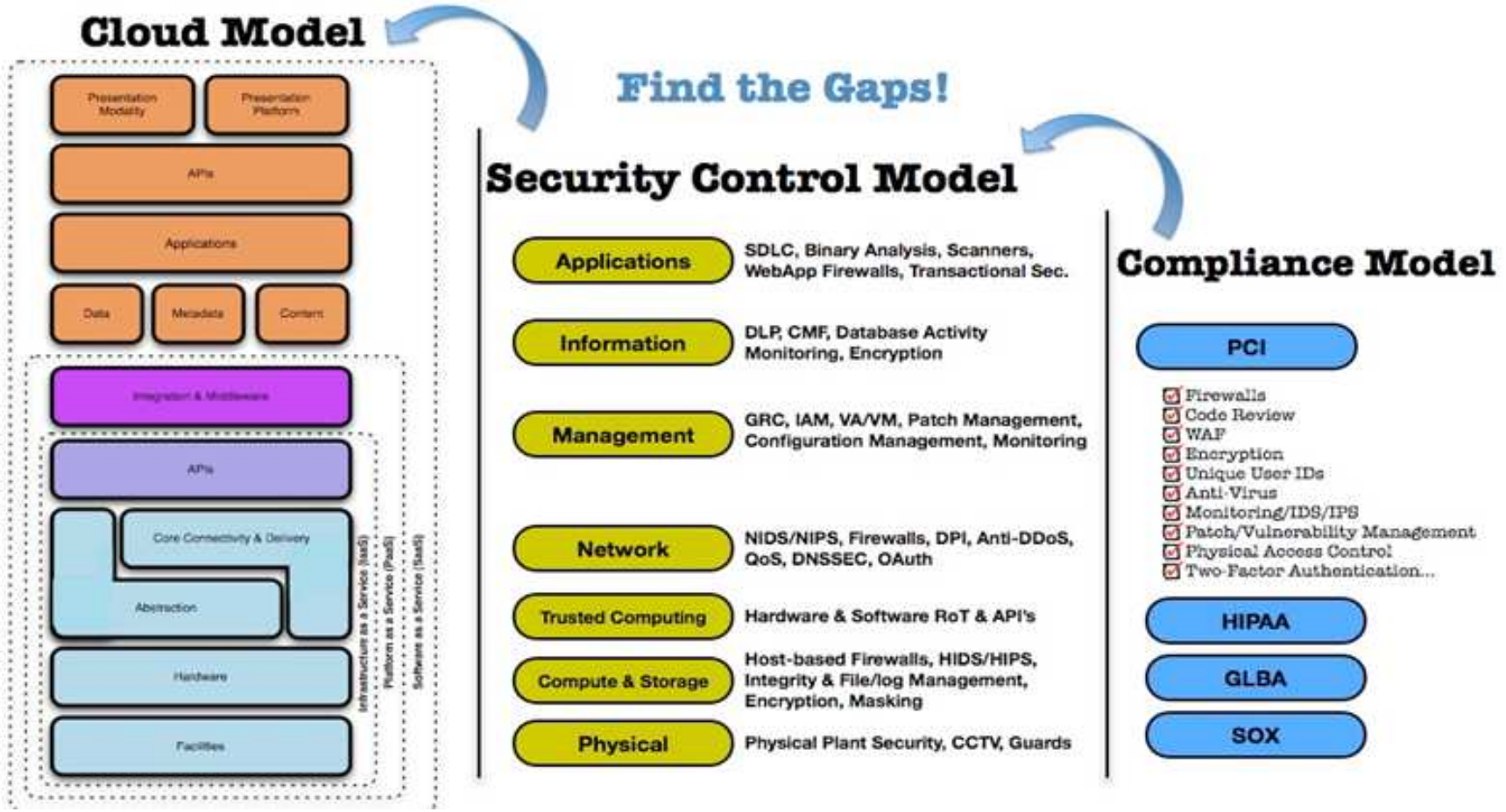
General Security Concept



NIST Reference Architecture



Cloud Security Model



CSA Notorious 9
Cloud Top Threats in 2013

1. **Data breaches/ leaks**
2. **Data loss**
3. Account or service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of services
6. Malicious Insiders
7. Cloud abuse
8. Insufficient due diligence
9. Shared technology vulnerabilities

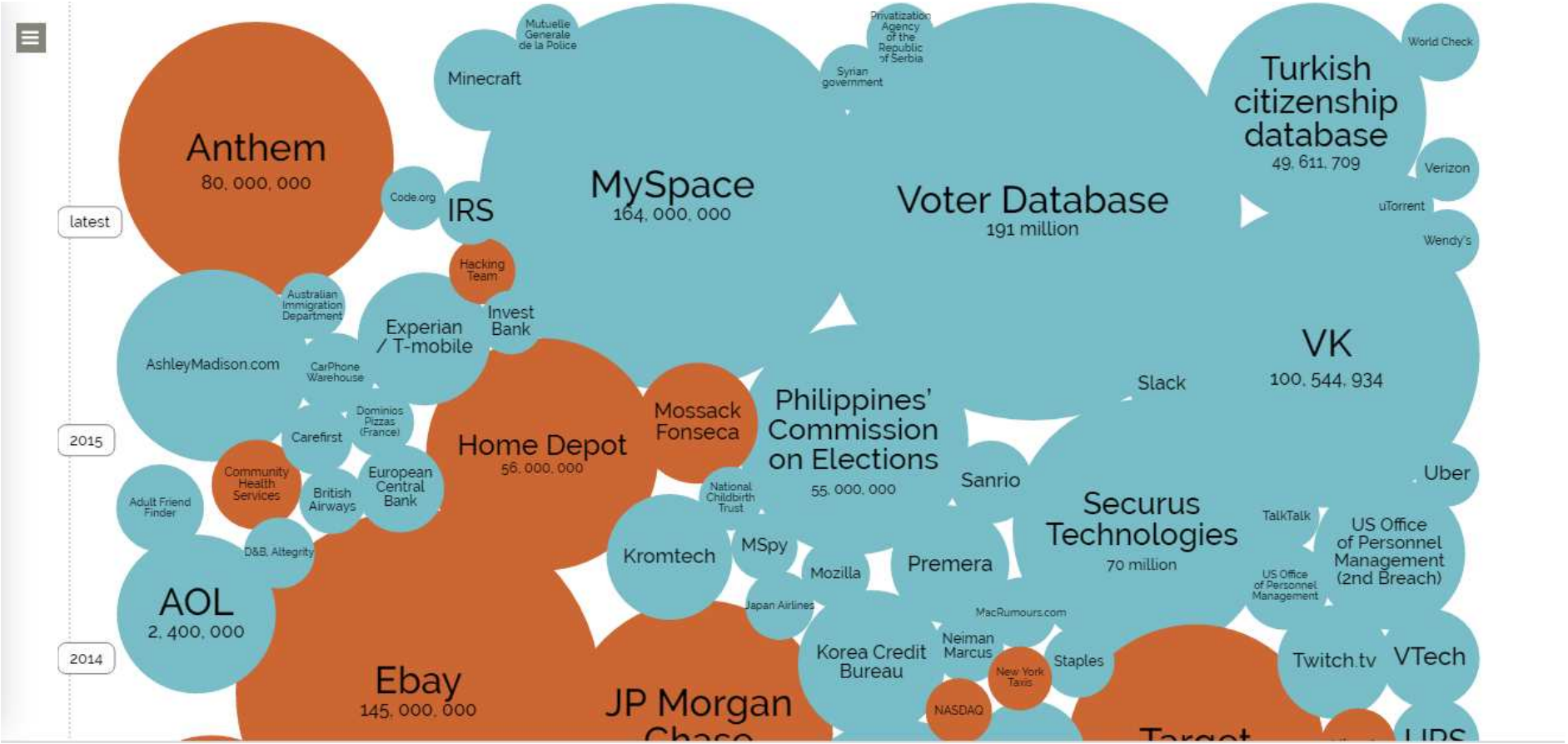
CSA Treacherous 12
Cloud Top Threats in 2016

1. **Data Breaches**
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. **Data Loss**
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

Data Breaches

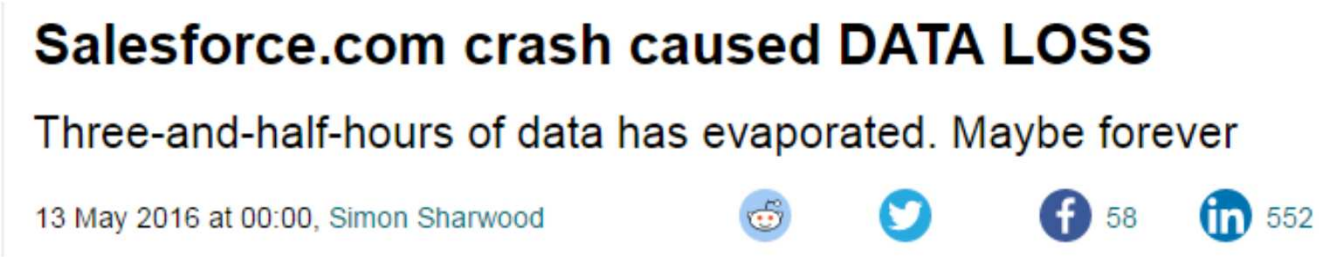
World's Biggest Data Breaches
Selected losses greater than 30,000 records (updated 11th July 2016)



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Data Loss

http://www.computerworld.com/article/2973600/cloud-computing/google-cloud-loses-data-belgium-itbwcw.html



http://www.theregister.co.uk/2016/05/13/salesforcecom_crash_caused_data_loss/

Data Security on Cloud

How to protect your data from being observed?

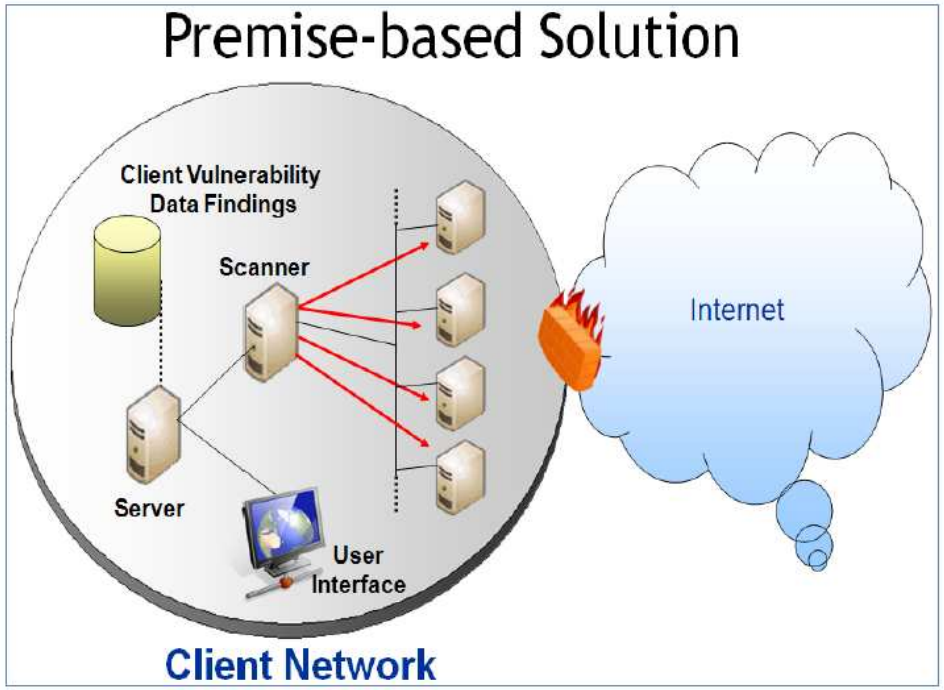
- Data Encryption
  - what about KEY? and Key Management?
  - encryption algorithm?

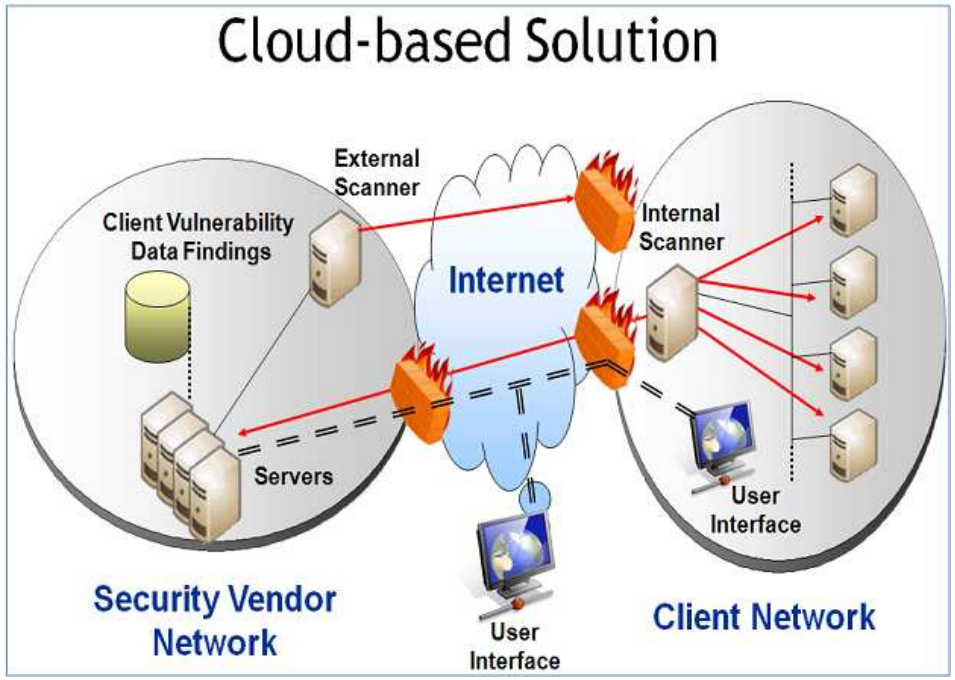
- Data Masking for Sensitive data like bank accounts
  - maintain a mapping between real and masked data

Data Life Cycle

https://securosis.com/tag/data+security+lifecycle

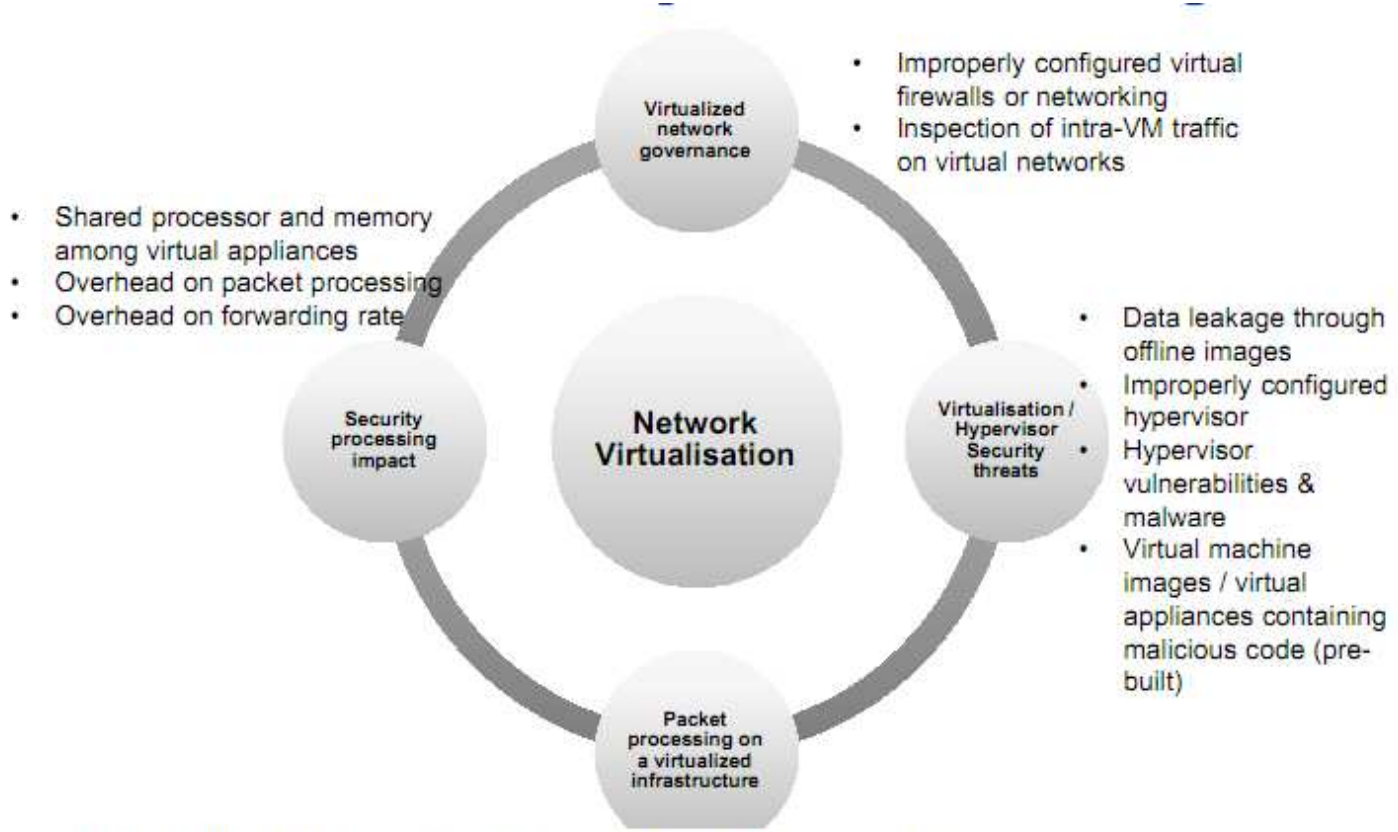
Cloud Threats and Vulnerabilities





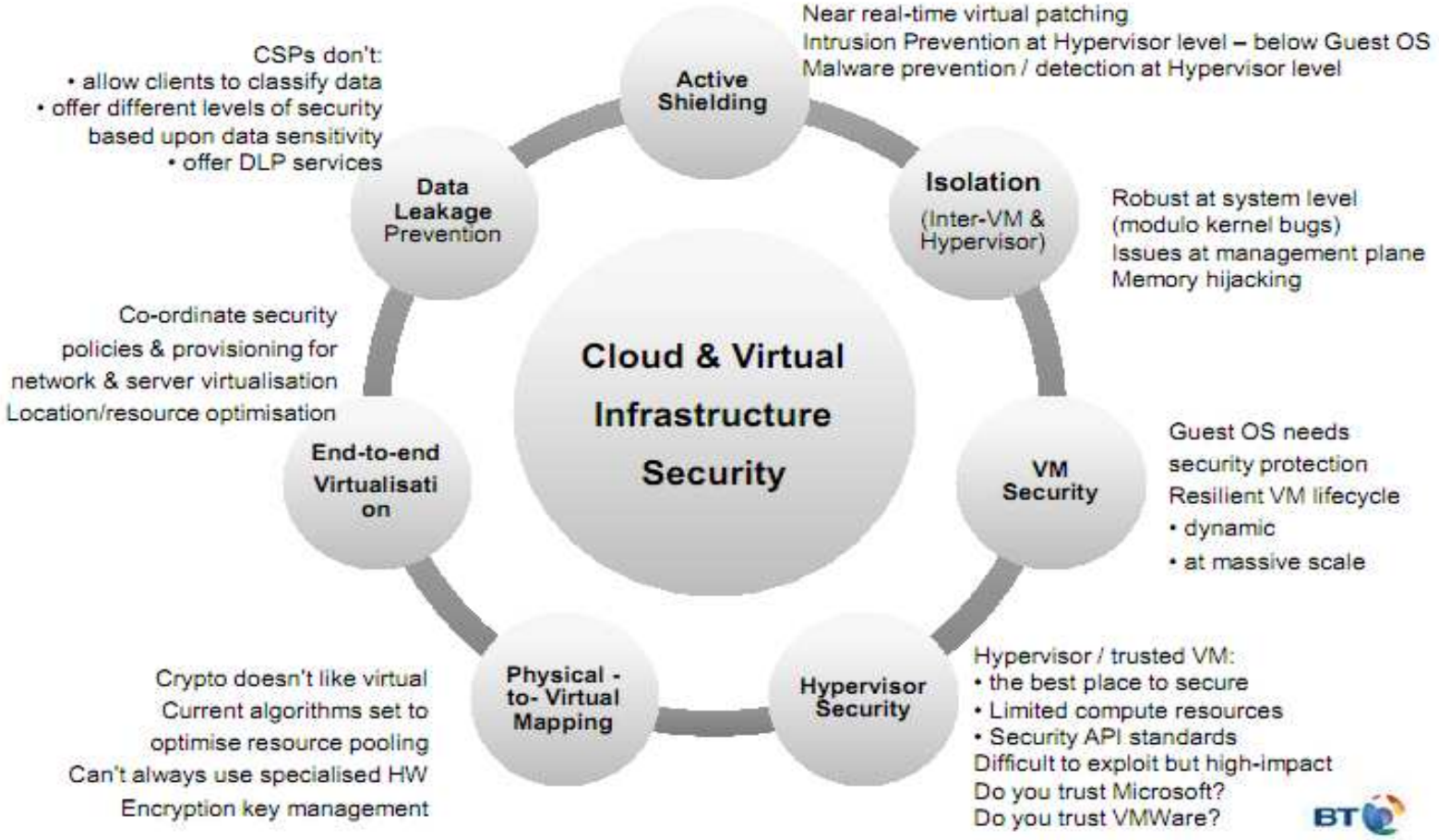
Adopted from "Realizing the Benefits of Vulnerability Management in the Cloud" by Gordon MacKay, CTO, Digital Defense, Inc.

Cloud Security Issues

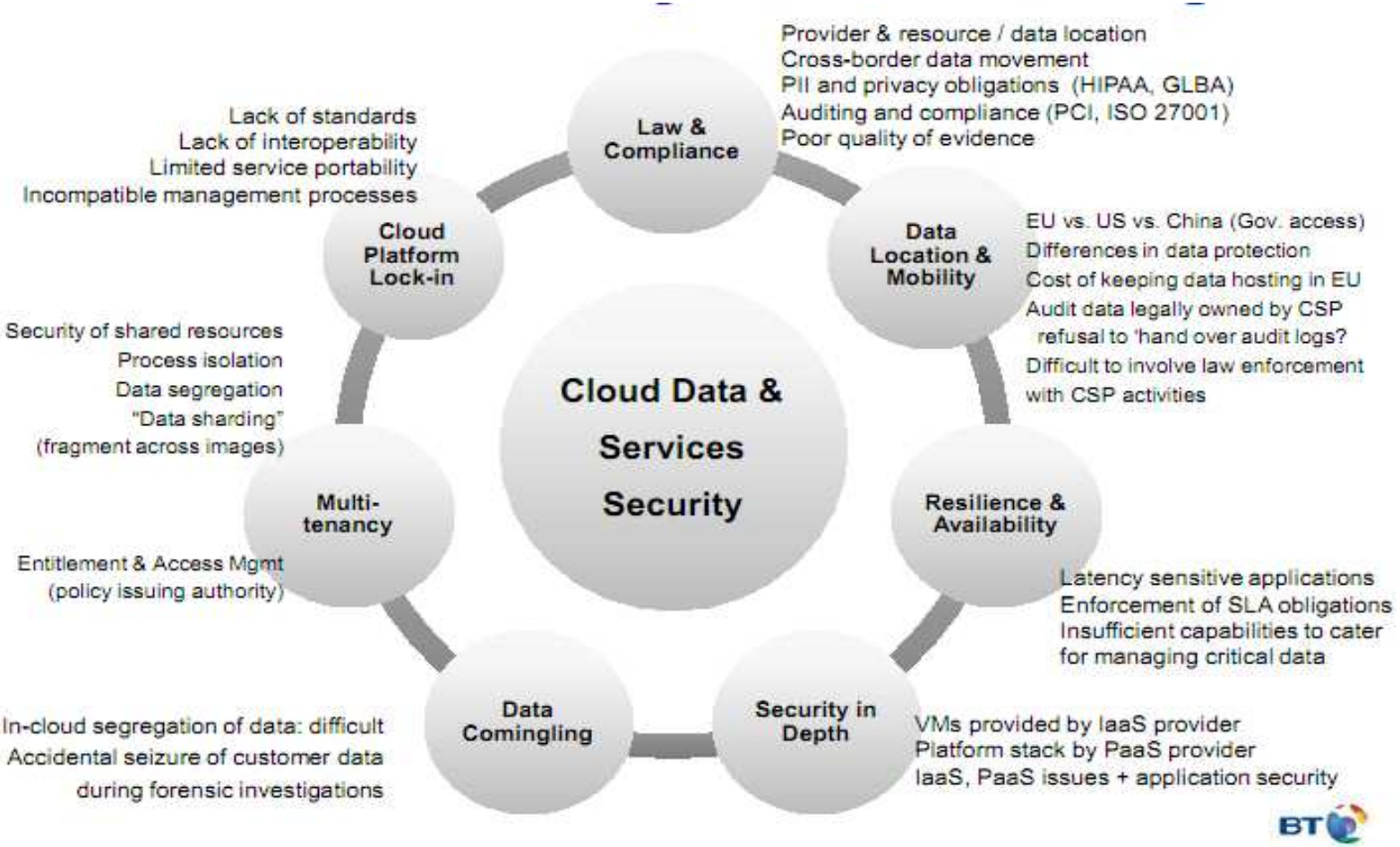


- Confidentiality → **efficient data encryption process & encrypted processing function**
- Integrity →**integrity monitoring: virtual image, network traffic & protocol processing ; accountability**
- Resource isolation → **bandwidth slicing ; virtual to physical mapping ; network processor scheduling**

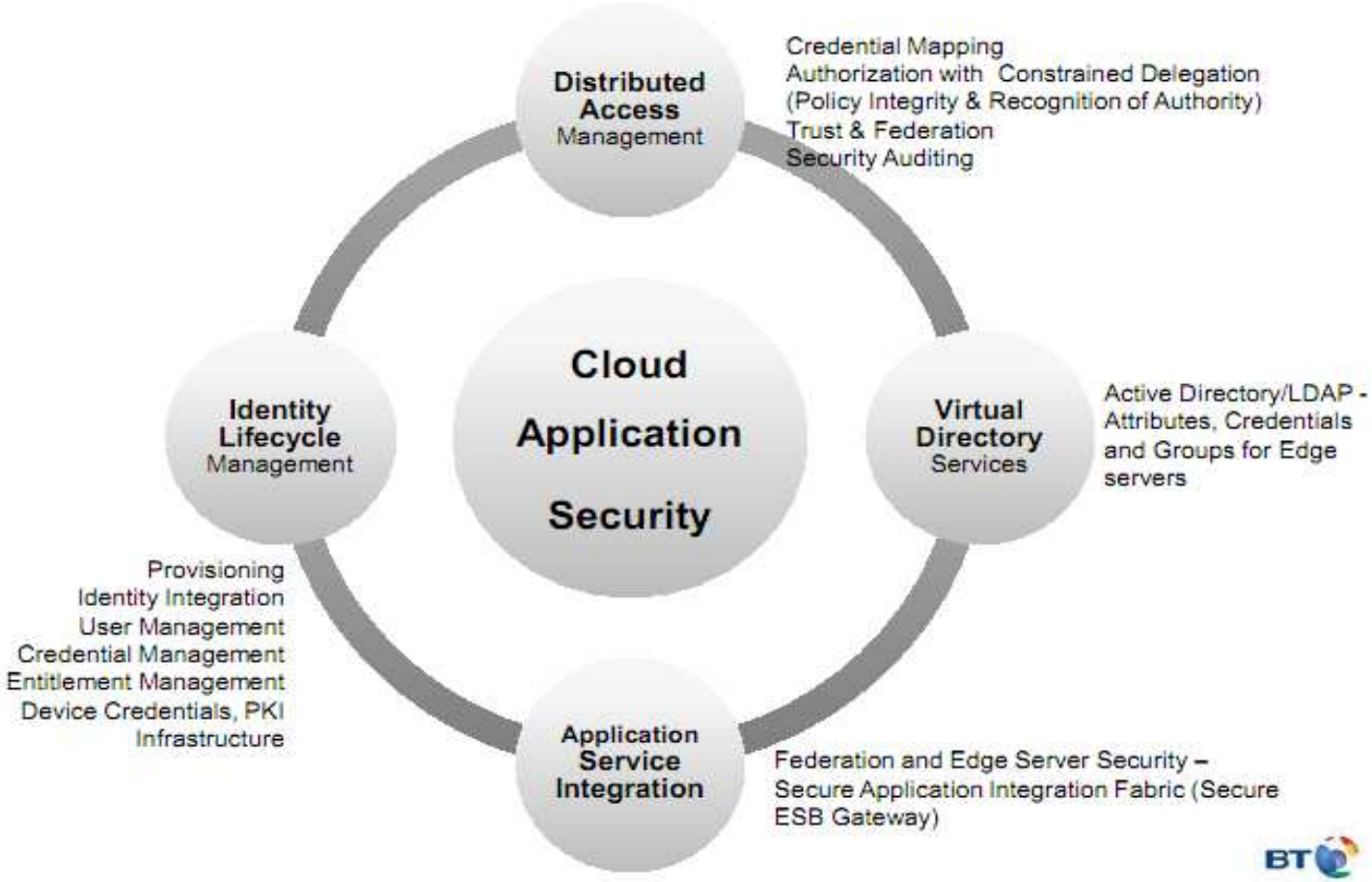
Cloud Security Issues



Cloud Security Issues



Cloud Security Issues



Q&A
Thank you