RSA®CONFERENCE
ASIA PACIFIC 2013

Security in knowledge

MA, I GOT ME A CLOUD TOO! BUILDING AND MANAGING A SECURE PRIVATE CLOUD.

PHORAM MEHTA CISSP, CISM
PAYPAL

KURT SAUER
PAYPAL

Session ID: CLD-T01

Session Classification: INTERMEDIATE

Agenda

- Why did you get a cloud: **Business Drivers**
- What is in your cloud: **Scope Definition**
- Where does your cloud sit: **Architecture**
- How to protect your cloud: **Risk Management**
- My neighbor's cloud: **References**

Business Drivers

- Easy Provisioning:
  - On-demand
  - Self-service
  - Automated
- Ubiquitous:
  - Multi-platform support
  - Broad network access
  - Multi-tenancy

Photo courtesy: contrib.andrew.cmu.edu

Business Drivers cont..

- Elasticity:
  - Quick Scale up
  - Resource release
  - Heterogeneous

- Accountability:
  - Measured usage
  - Optimization
  - Monitoring/Reporting

Courtesy – wordle.net

Secure Cloud Drivers

- An Opportunity
  - Fresh start you always wanted
  - Design your dream network
  - Shoot for the Sun
- Standardization
- Accountability
  - Clear roles and responsibilities
  - Auditing and Monitoring
- Compliance Automation
- Governance

Photo courtesy: forbes.com

Scope Definition

- Asset Identification
  - Applications
  - Data
  - Processes
  - Users
- Business Impact
  - Portfolio IA
  - Continuity Plan
- Information Flow

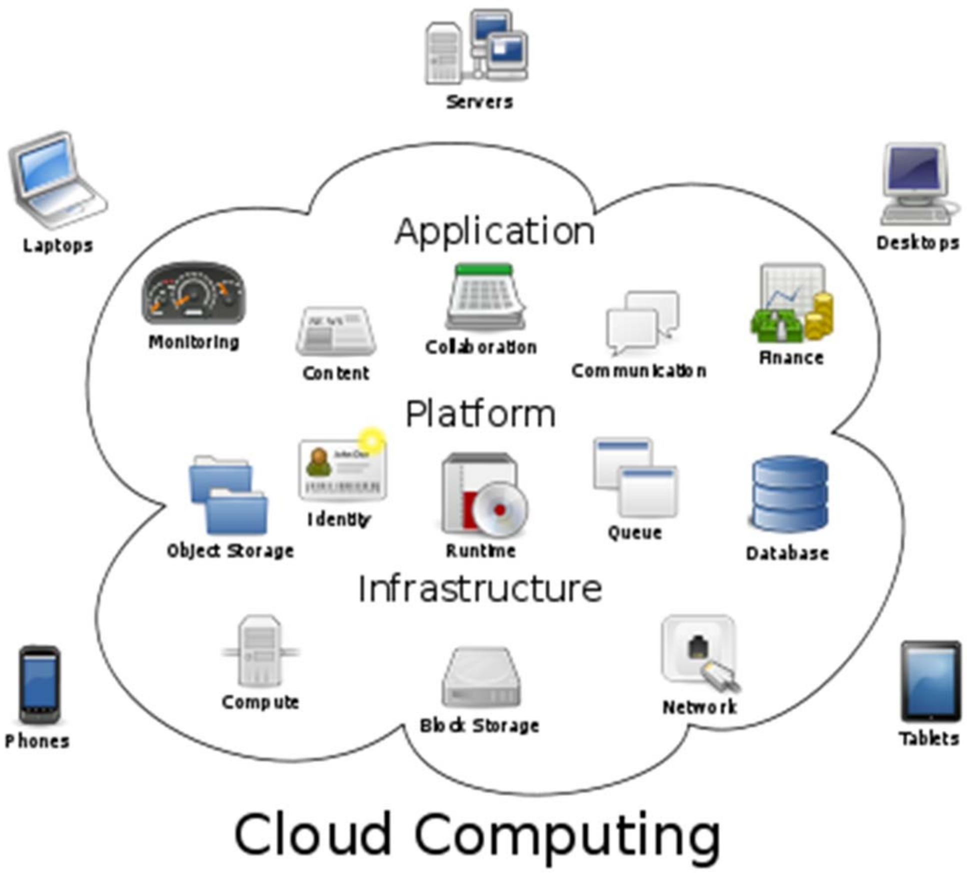


Photo courtesy: nailab.co.ke

Architecture

- Demarcation: Intranet vs Extranet
- Roles and responsibilities
- Deployment Model
  - SaaS
  - PaaS
  - IaaS
  - Custom

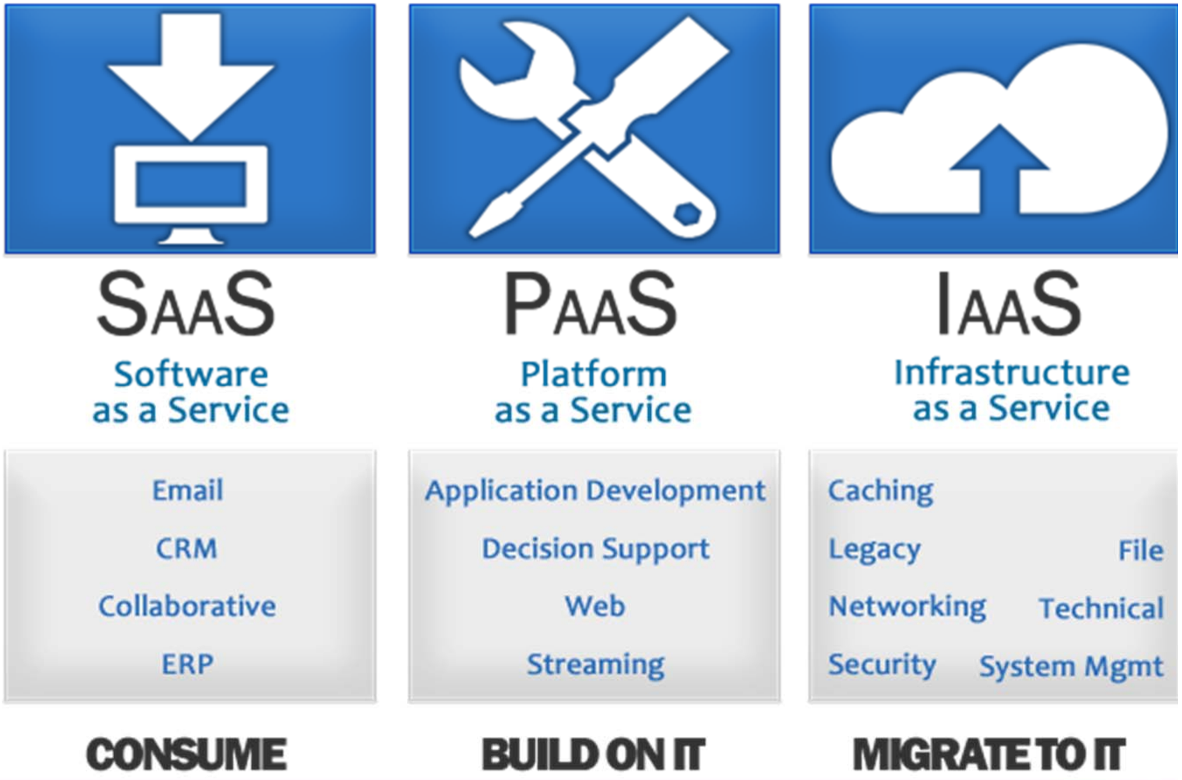


Photo courtesy:thumbsup.in.th

Risk Management

- Compliance and Audit
- Privacy and Legal
- Incident Response
- BCP/DR
- Security Operations & Monitoring
- Cryptographic Controls
- Data Security
- Access Administration (IdAM)
- Network Segmentation
- Application Security

Security in Depth/Layers

- Trust Zones
- Platform Hardening
- AuthN & AuthZ
- Data Control
- Virtualization
- Event Analytics

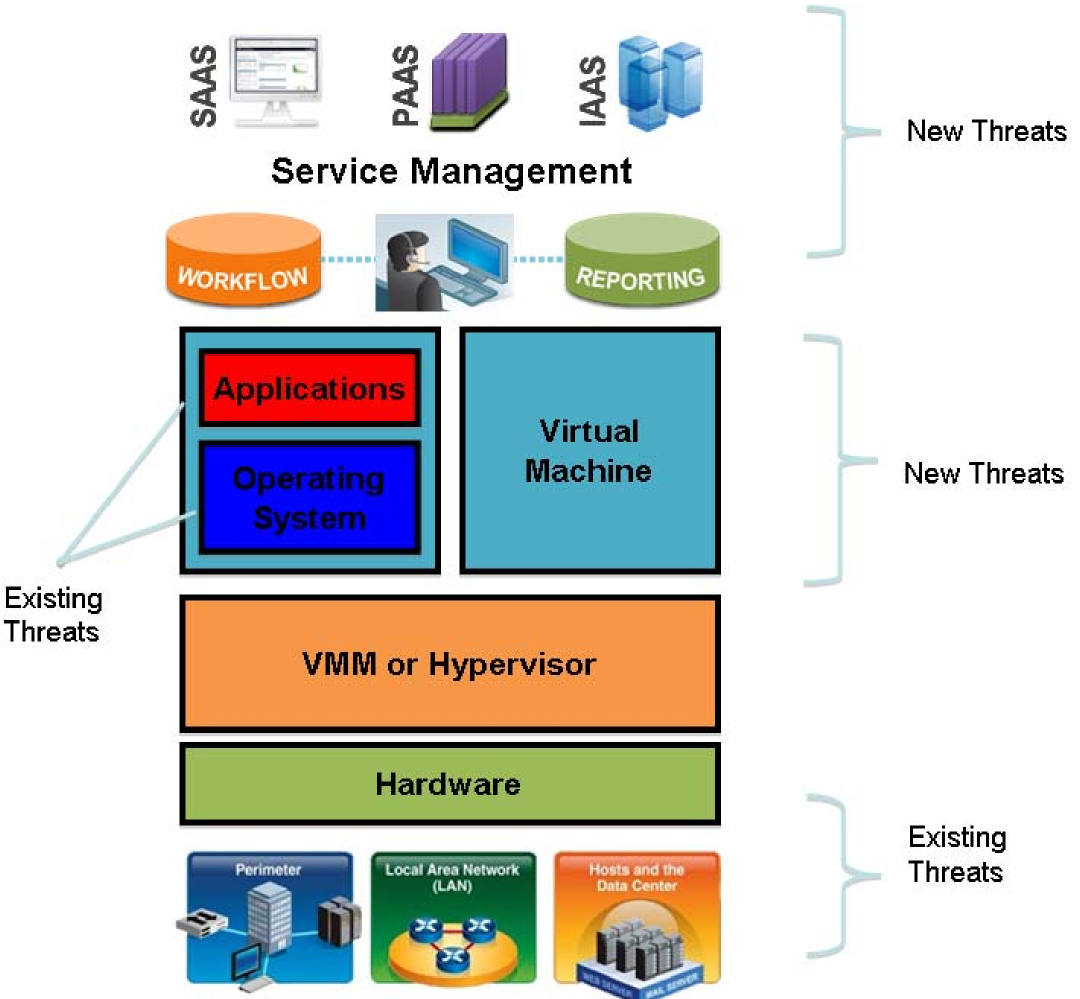
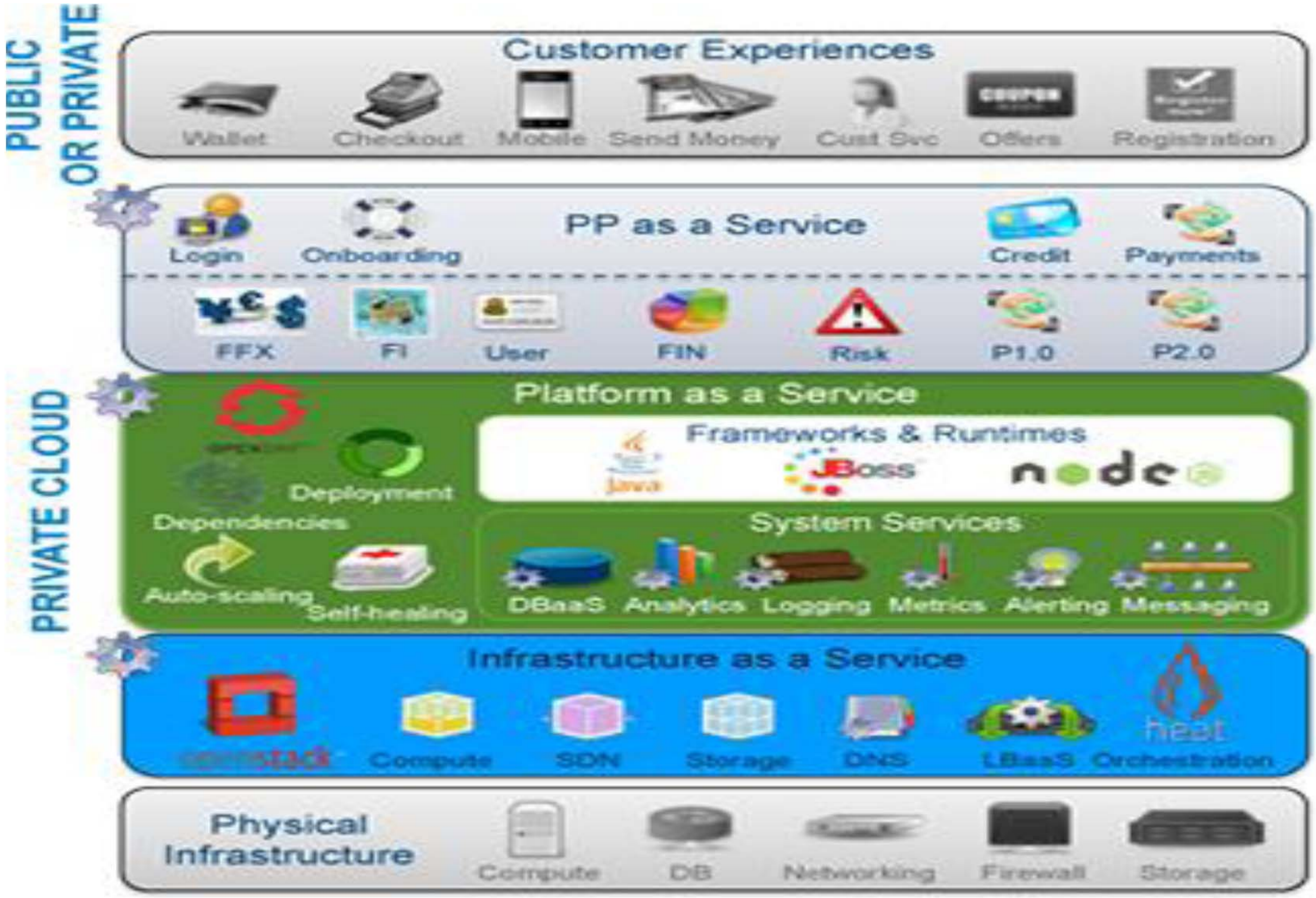
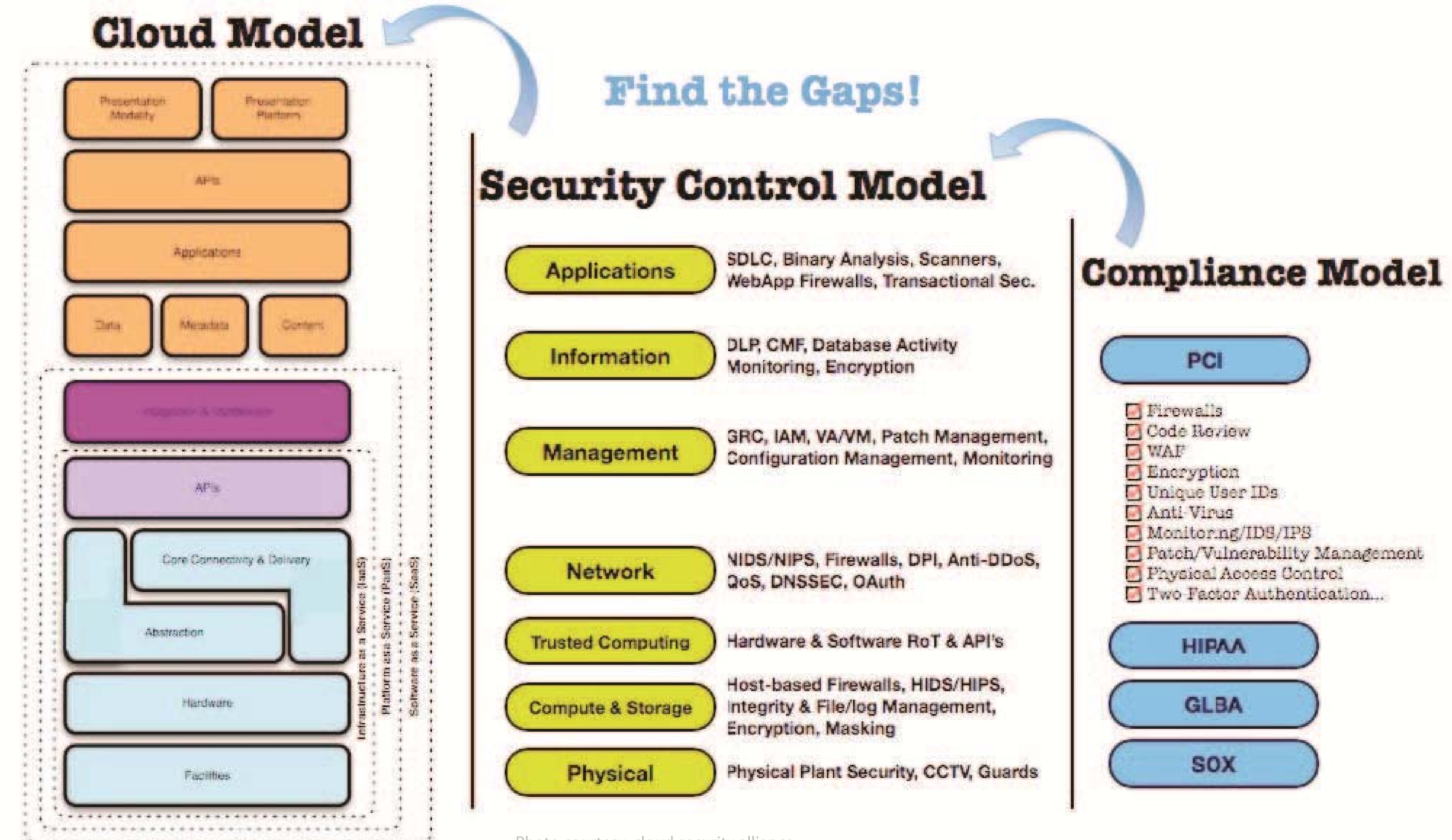


Photo courtesy: IBM

Reference Architecture



Cloud Security Model



Cloud Model

Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two Factor Authentication...

HIPAA

GLBA

SOX

Photo courtesy: cloud security alliance

Resources

- Before Starting:
  - CSA Security Guidance: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
  - Cloud Security Readiness Tool: http://technet.microsoft.com/en-us/security/jj554736.aspx?ppud=4

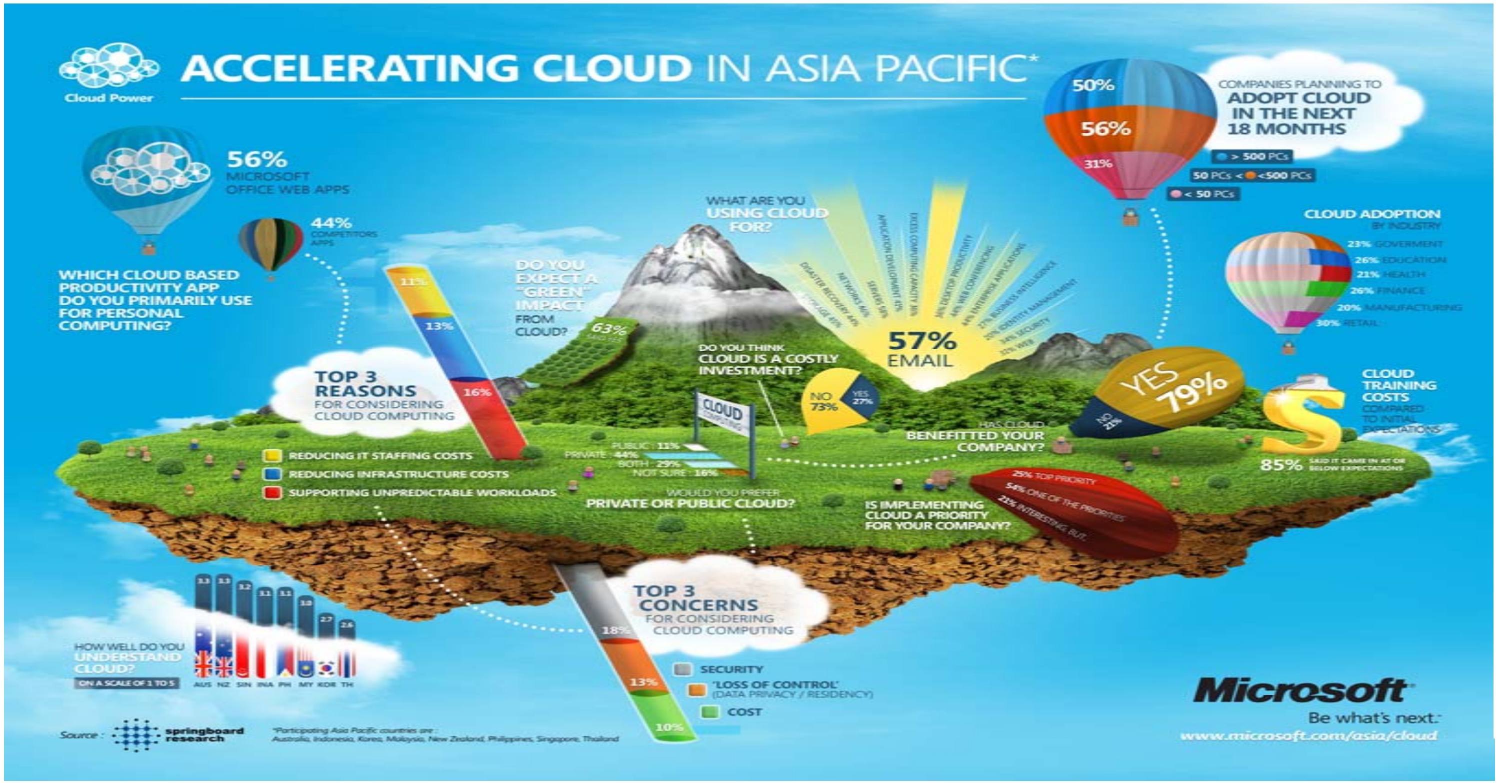
- After Starting:
  - CAESARS: http://www.dhs.gov/continuous-asset-evaluation-situational-awareness-and-risk-scoring-reference-architecture-report
  - Japan Information Security Audit Association: http://jasa.jp/information/result.html

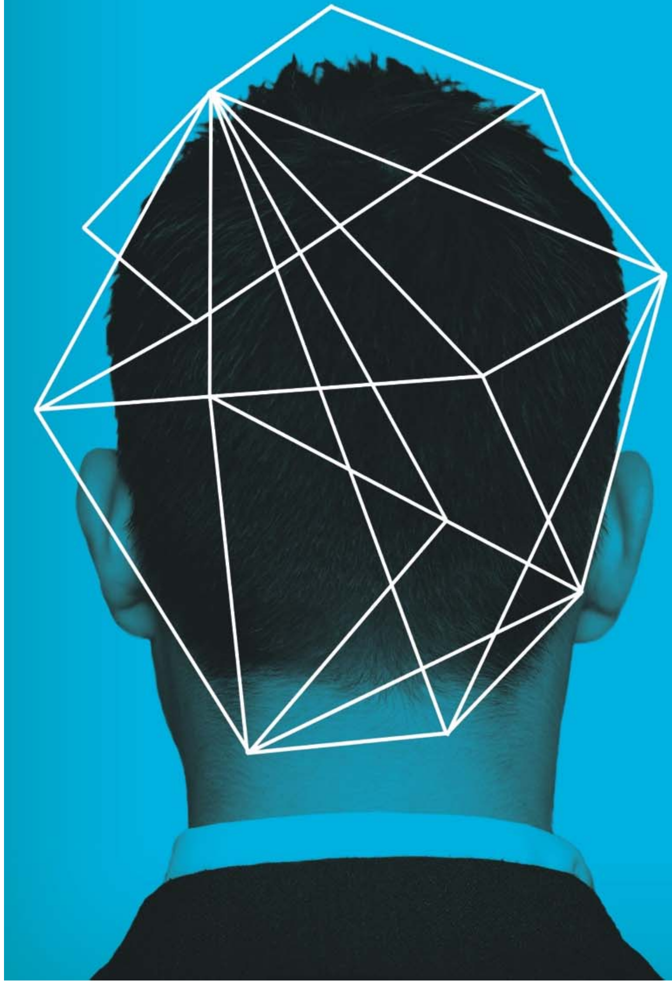
Other Resources

- Links to industry resources:
  - NIST: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505
  - Open Security Architecture: http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing
  - CSA Cloud Control Matrix: https://cloudsecurityalliance.org/research/ccm/
  - ISACA Cloud Security Guidance: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx

Recap

- DENTIFY the Drivers
- DEFINE the Scope
- ESTABLISH a Security Framework
- ADDRESS key Risks


ACCELERATING CLOUD IN ASIA PACIFIC*
Cloud Power
56%
MICROSOFT OFFICE WEB APPS
44%
COMPETITORS APPS
WHICH CLOUD BASED PRODUCTIVITY APP DO YOU PRIMARILY USE FOR PERSONAL COMPUTING?
11%
13%
16%
TOP 3 REASONS FOR CONSIDERING CLOUD COMPUTING
REDUCING IT STAFFING COSTS
REDUCING INFRASTRUCTURE COSTS
SUPPORTING UNPREDICTABLE WORKLOADS
DO YOU EXPECT A "GREEN" IMPACT FROM CLOUD?
63% SAID YES
WHAT ARE YOU USING CLOUD FOR?
STORAGE 45%
DISASTER RECOVERY 44%
NETWORKS 46%
SERVERS 50%
APPLICATION DEVELOPMENT 45%
EXCESS COMPUTING CAPACITY 38%
36% DESKTOP PRODUCTIVITY
44% WEB CONFERENCING
44% ENTERPRISE APPLICATIONS
27% BUSINESS INTELLIGENCE
20% IDENTITY MANAGEMENT
34% SECURITY
32% WEB
57% EMAIL
DO YOU THINK CLOUD IS A COSTLY INVESTMENT?
NO 73%
YES 27%
CLOUD COMPUTING
PUBLIC : 11%
PRIVATE : 44%
BOTH : 29%
NOT SURE : 16%
WOULD YOU PREFER PRIVATE OR PUBLIC CLOUD?
HAS CLOUD BENEFITTED YOUR COMPANY?
YES 79%
NO 21%
IS IMPLEMENTING CLOUD A PRIORITY FOR YOUR COMPANY?
25% TOP PRIORITY
54% ONE OF THE PRIORITIES
21% INTERESTING BUT..
50%
56%
31%
COMPANIES PLANNING TO ADOPT CLOUD IN THE NEXT 18 MONTHS
> 500 PCs
50 PCs < <500 PCs
< 50 PCs
CLOUD ADOPTION BY INDUSTRY
23% GOVERMENT
26% EDUCATION
21% HEALTH
26% FINANCE
20% MANUFACTURING
30% RETAIL
CLOUD TRAINING COSTS COMPARED TO INITIAL EXPECTATIONS
85% SAID IT CAME IN AT OR BELOW EXPECTATIONS
3.3
3.3
3.2
3.1
3.1
3.0
2.7
2.6
AUS NZ SIN INA PH MY KOR TH
HOW WELL DO YOU UNDERSTAND CLOUD?
ON A SCALE OF 1 TO 5
18%
13%
10%
TOP 3 CONCERNS FOR CONSIDERING CLOUD COMPUTING
SECURITY
'LOSS OF CONTROL' (DATA PRIVACY / RESIDENCY)
COST
Source : springboard research
*Participating Asia Pacific countries are : Australia, Indonesia, Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand
Microsoft
Be what's next.
www.microsoft.com/asia/cloud



Phoram Mehta
phmehta@paypal.com