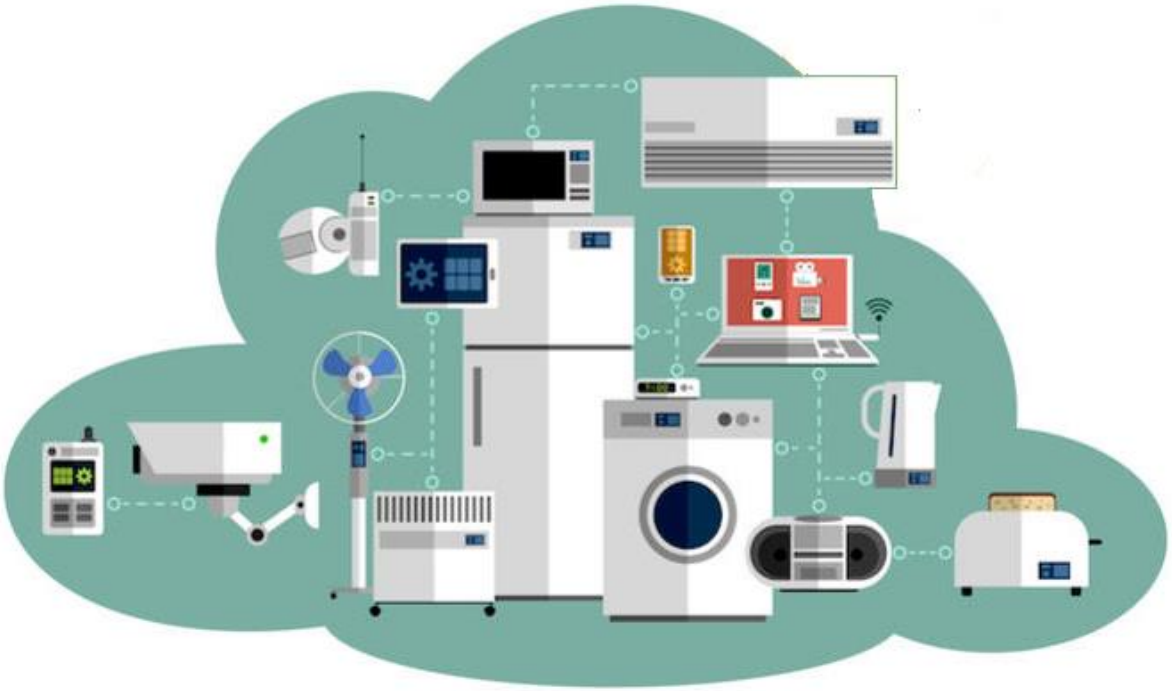
Assoc. Prof. Dr. Selvakumar Manickam

selva@usm.my

Now, Internet is moving to everyday objects & devices



This is what a 5ME
1956 (note:

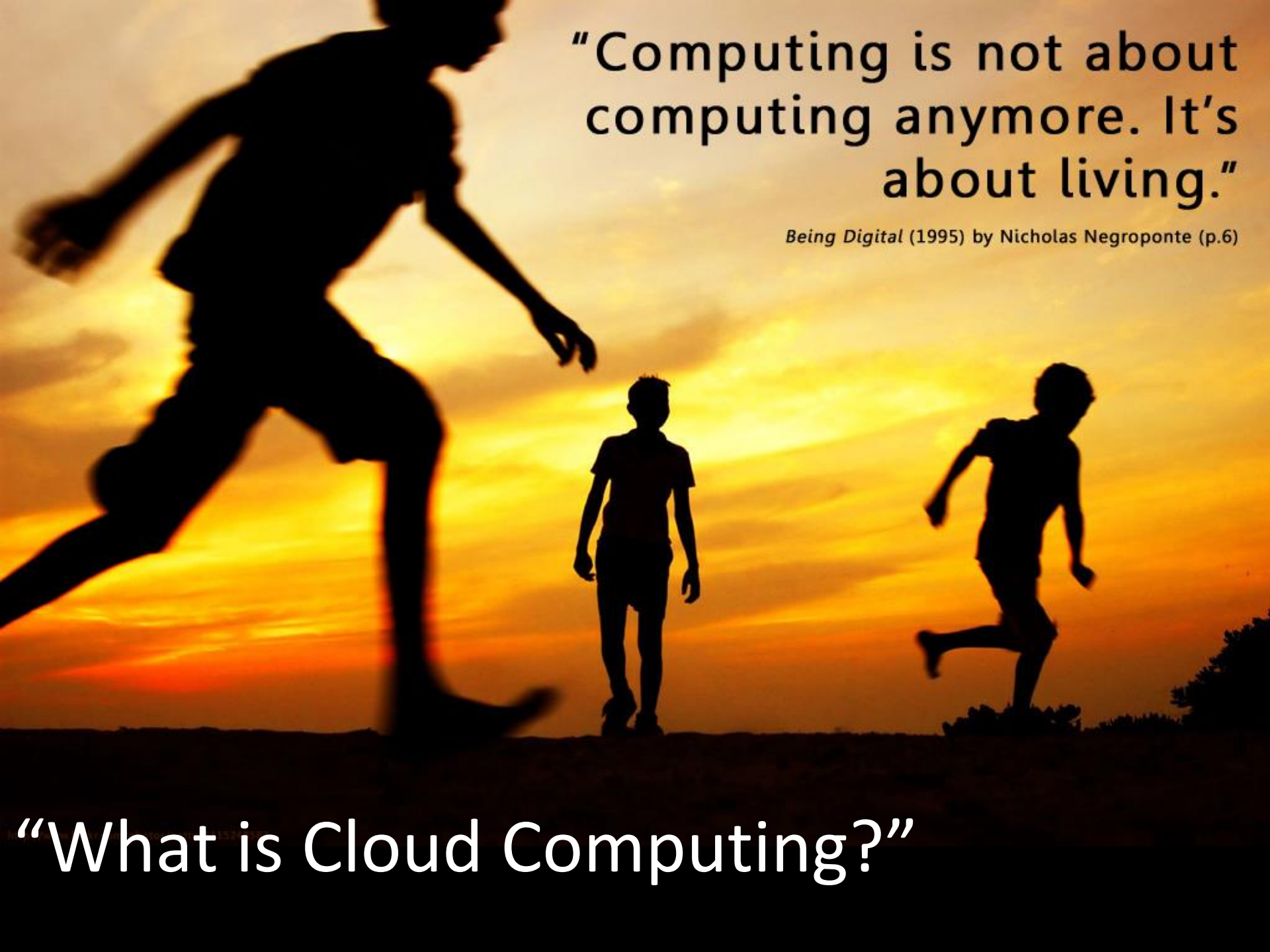

YOU'RE PRETTY NEW TO CLOUD STORAGE, AREN'T YOU?
LYNCH

A Massive Concentration of Resources

- "Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources"
- Also a massive concentration of risk
  - expected loss from a single breach can be significantly larger
  - concentration of "users" represents a concentration of threats
- "Ultimately, you can outsource responsibility but you can't outsource accountability."

Many Cloud Providers

- AWS: Amazon Web Services
  - EC2: Elastic Compute Cloud
  - S3: Simple Storage Service
  - EBS: Elastic Block Storage
- Microsoft Azure
- Ali Cloud
- Google Compute Engine
- Rightscale, Salesforce, EMC, Gigaspaces, 10gen, Datastax, Oracle, VMWare, Yahoo, Cloudera
- And many many more!



"What is Cloud Computing?"

Computing Models

- Cloud
- Grid
- Cluster
- Fog
- Distributed
- Edge
- Ambient
- Mist
- Serverless

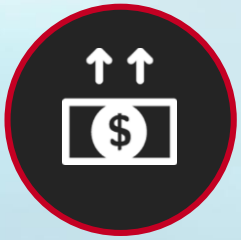
The cloud is one of the largest shifts in IT over the past decade, fueling innovation across the globe.

Today, it powers many businesses and mission-critical applications, allowing organizations to take advantage of its inherent flexibility.

It’s Time to Move to the Cloud

$200B

Gartner estimates cloud-related spend to exceed by 2016.

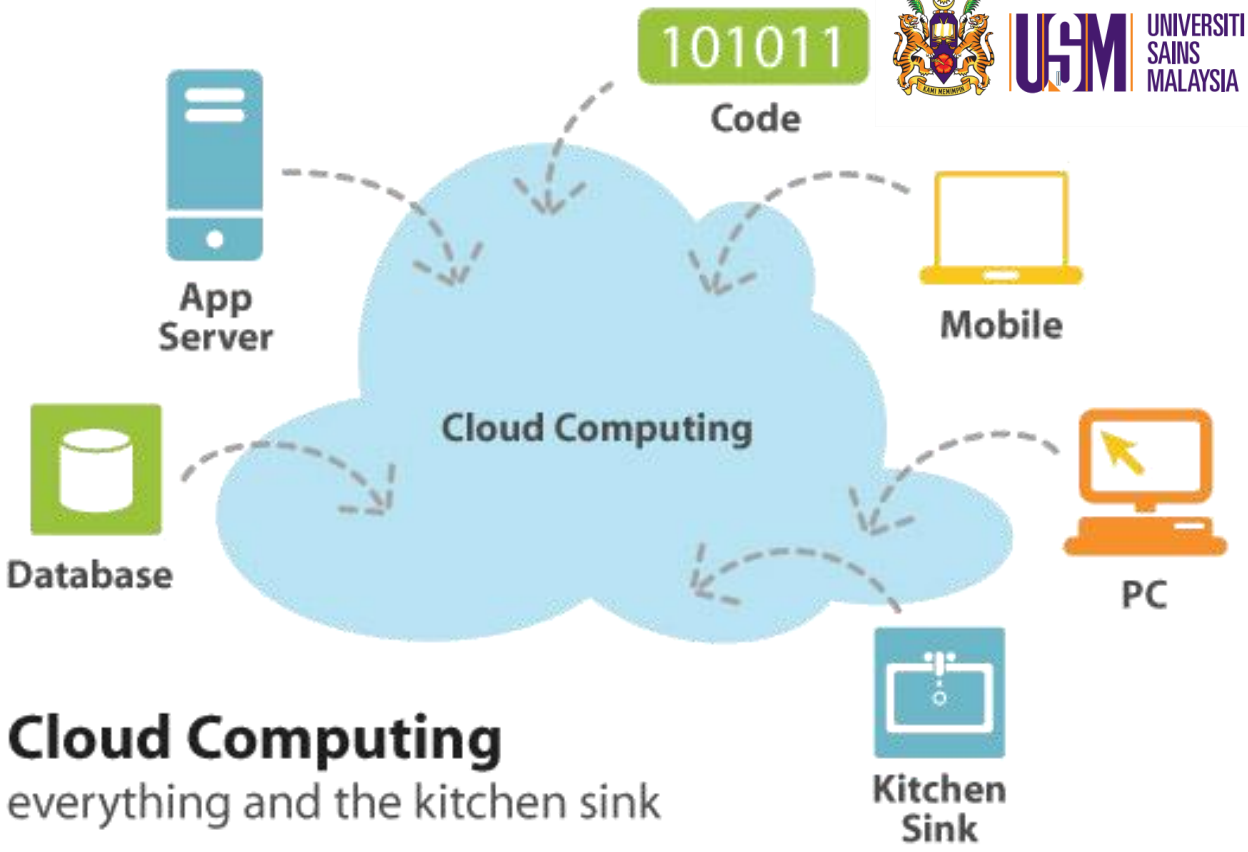


90%

of new spending in the next six years will be cloud-based.

87%

of businesses are using public cloud.



Common implies multi-tenancy, not single or isolated tenancy

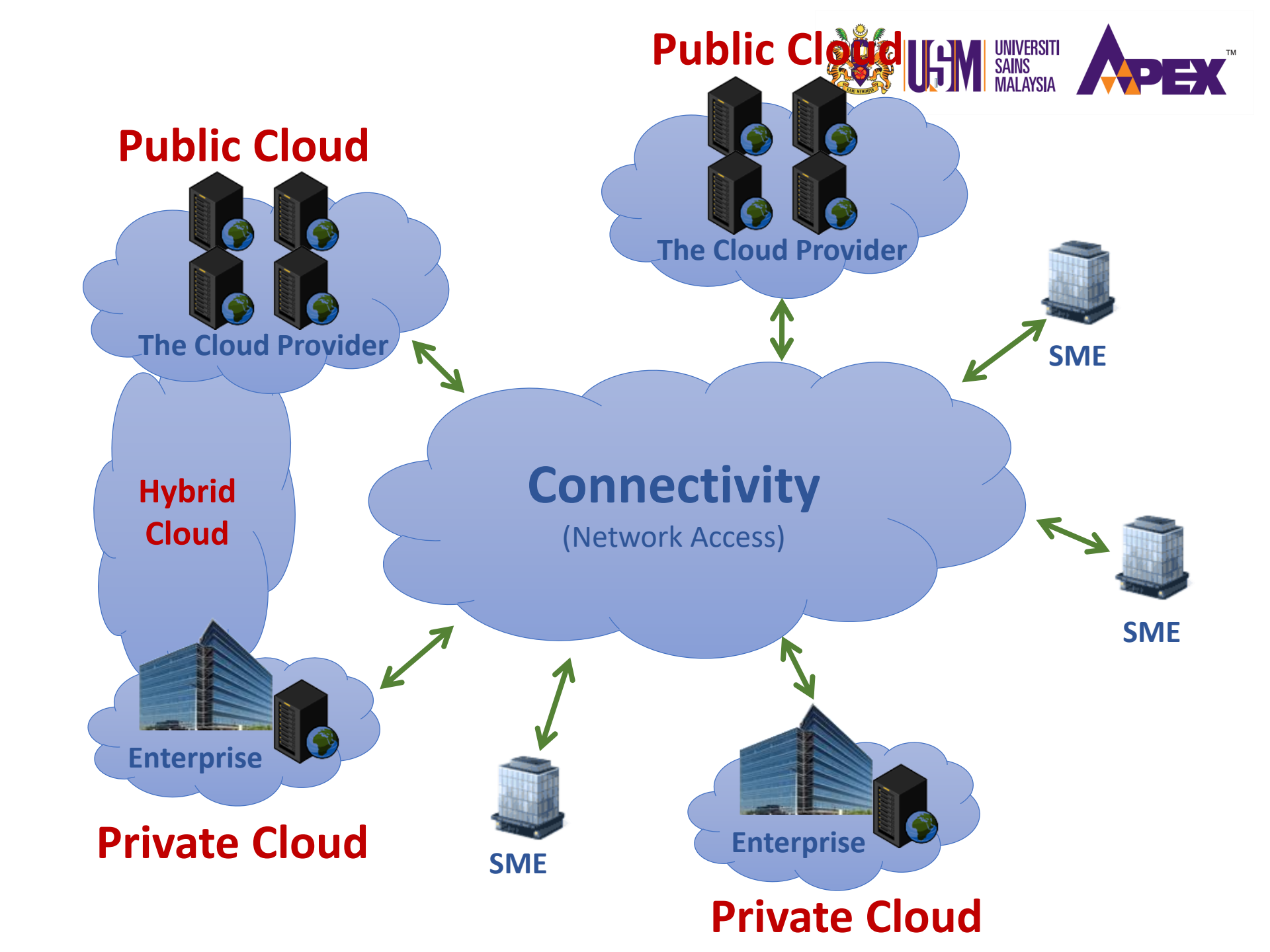
Location-independent

Online

Utility implies pay-for-use pricing

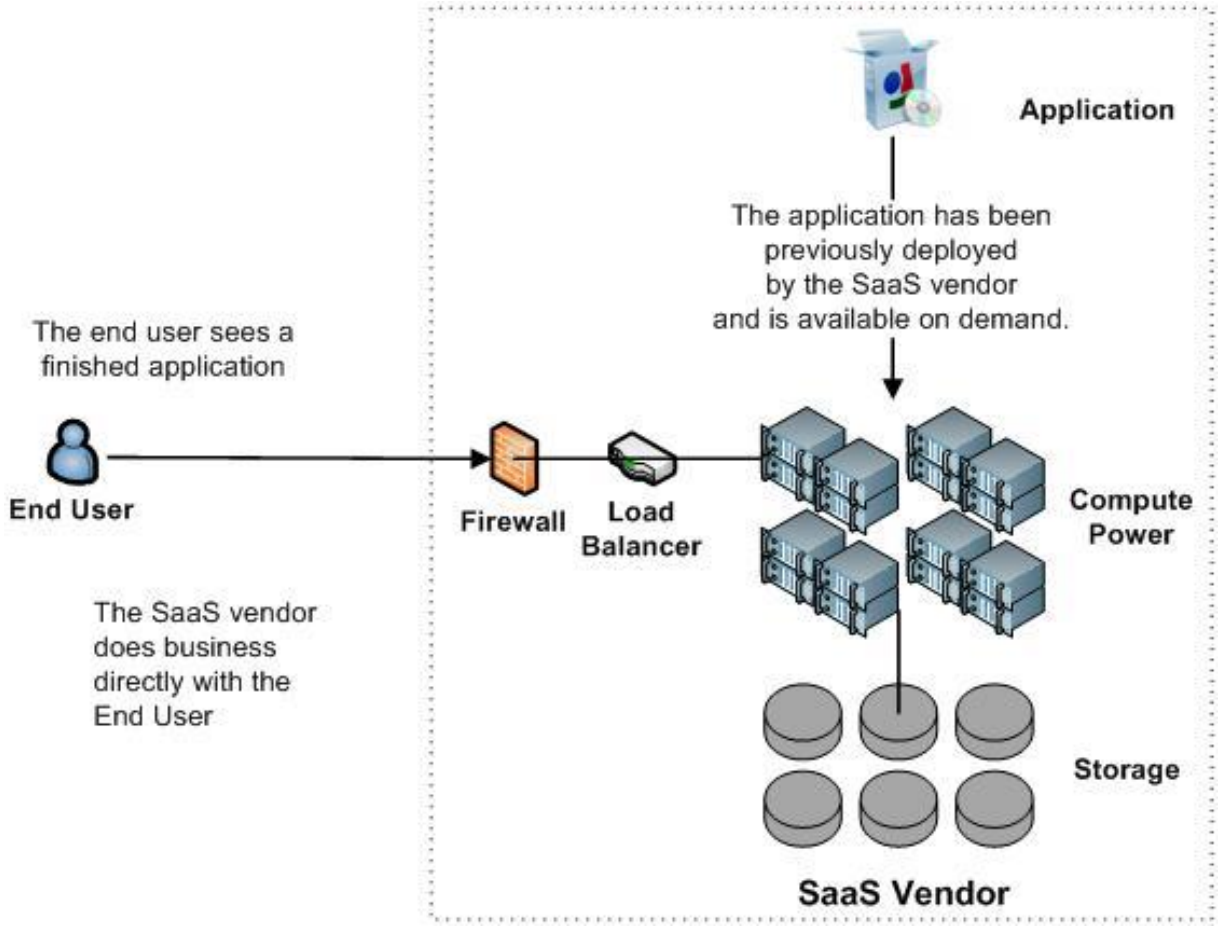
Demand implies ~infinite, ~immediate, ~invisible scalability

Cloud Computing Infrastructure Models


Public Cloud
Public Cloud
The Cloud Provider
The Cloud Provider
SME
Hybrid Cloud
Connectivity
(Network Access)
SME
Enterprise
SME
Enterprise
Private Cloud
Private Cloud

Architectural Layers of Cloud Computing

Software as a Service (SaaS)



salesforce.com
Success On Demand.

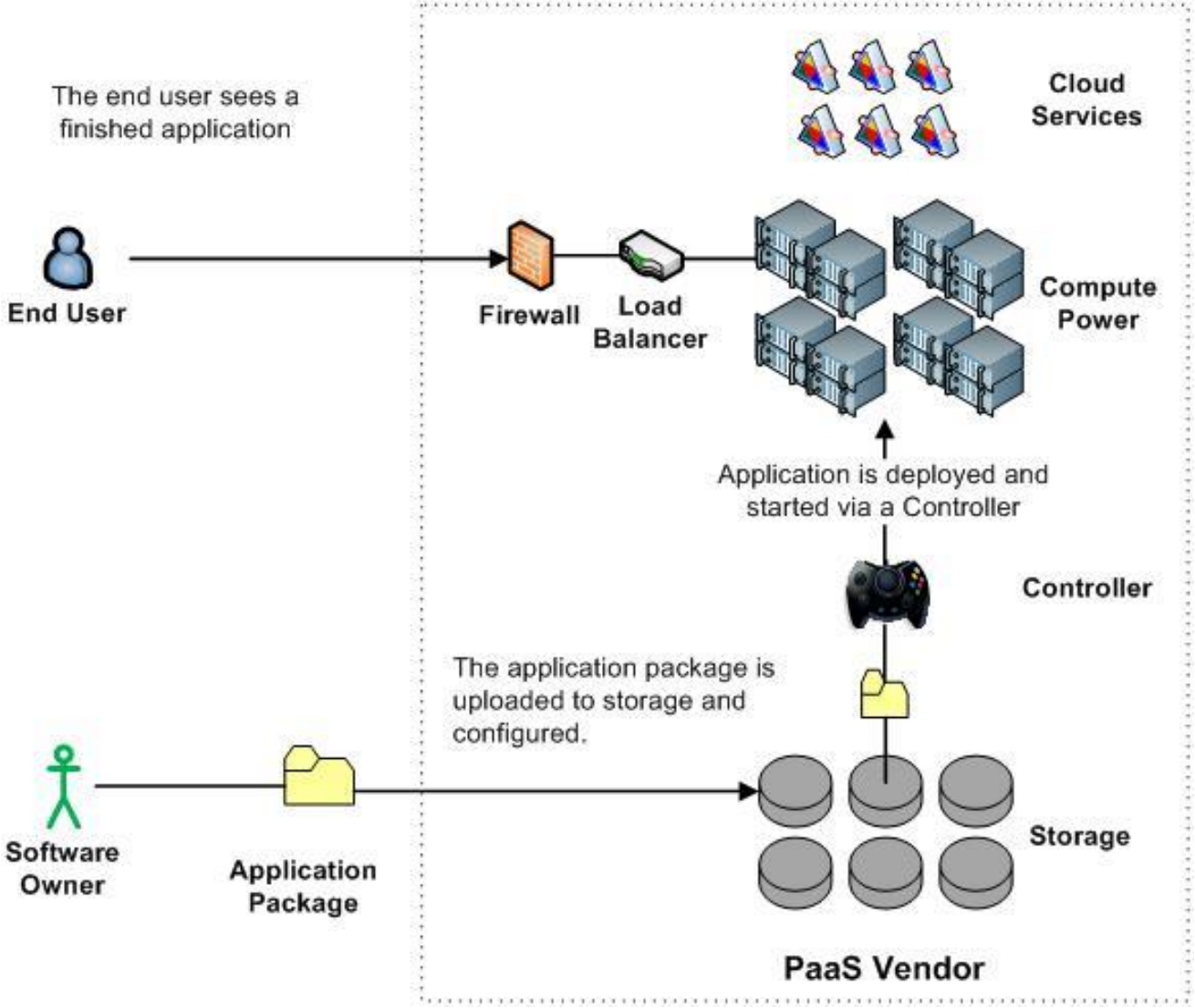
ZOHO
Work. Online

sliderocket

clarizen
Projects Made Real

Google Docs

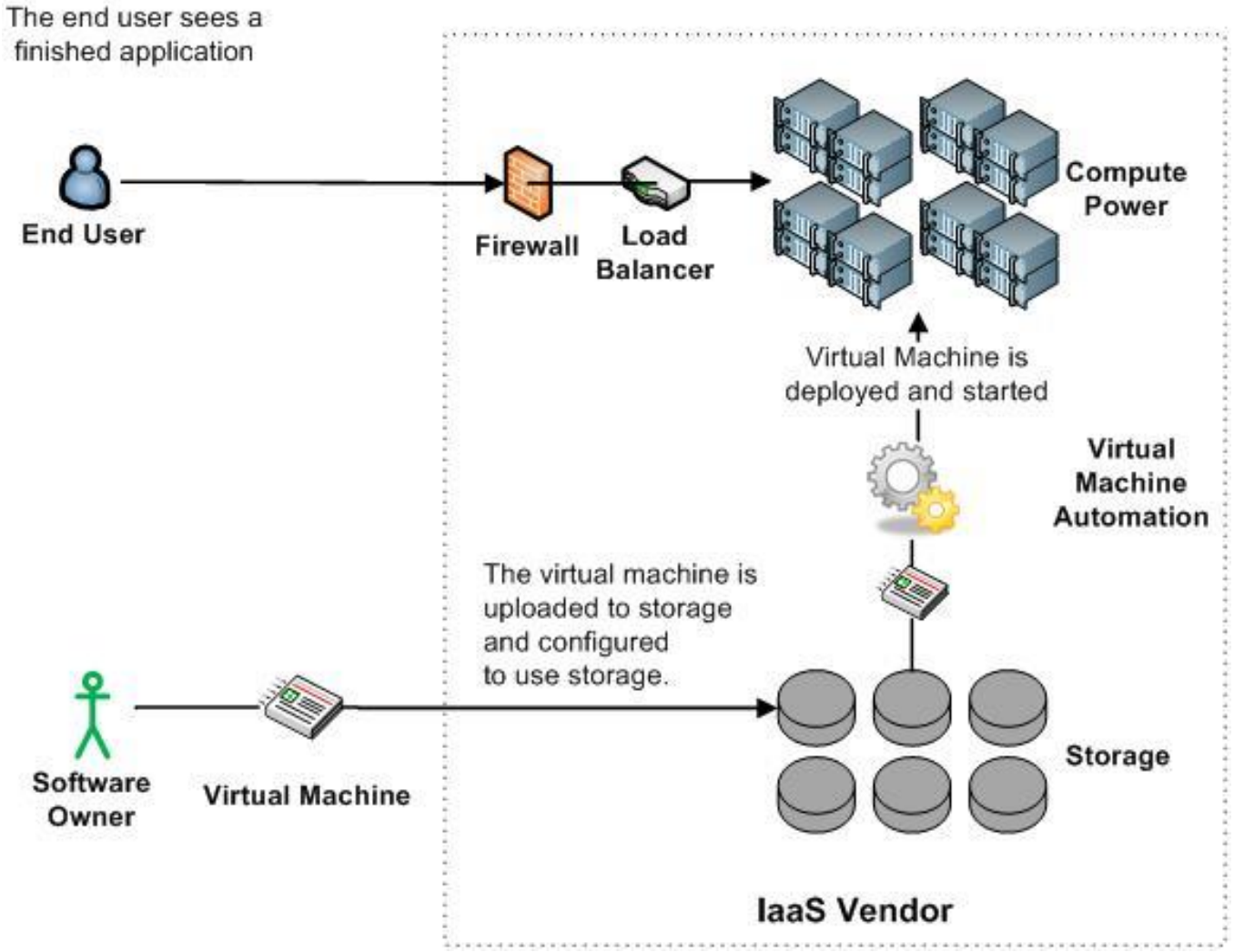
Platform as a Service (PaaS)



Google App Engine

Windows Azure

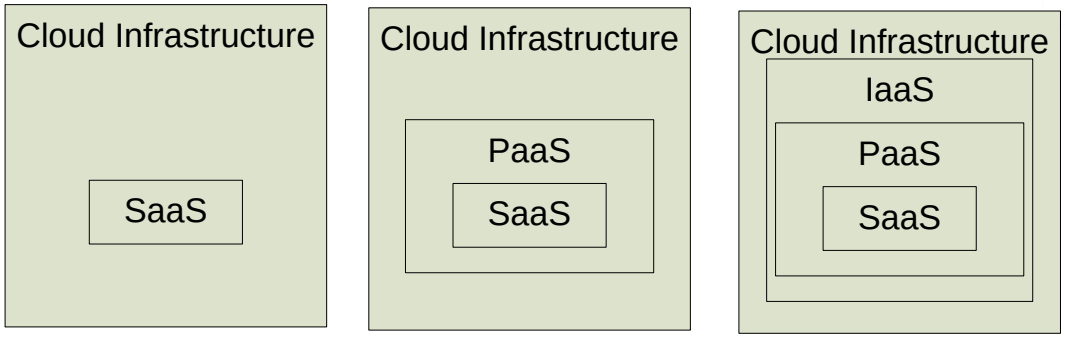
Infrastructure as a Service (IaaS)



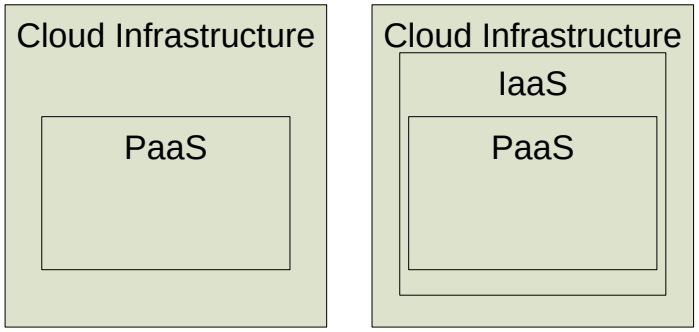
amazon web services™

rackspace

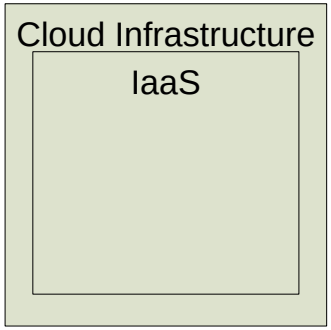
ServePath



Software as a Service (SaaS) Architectures



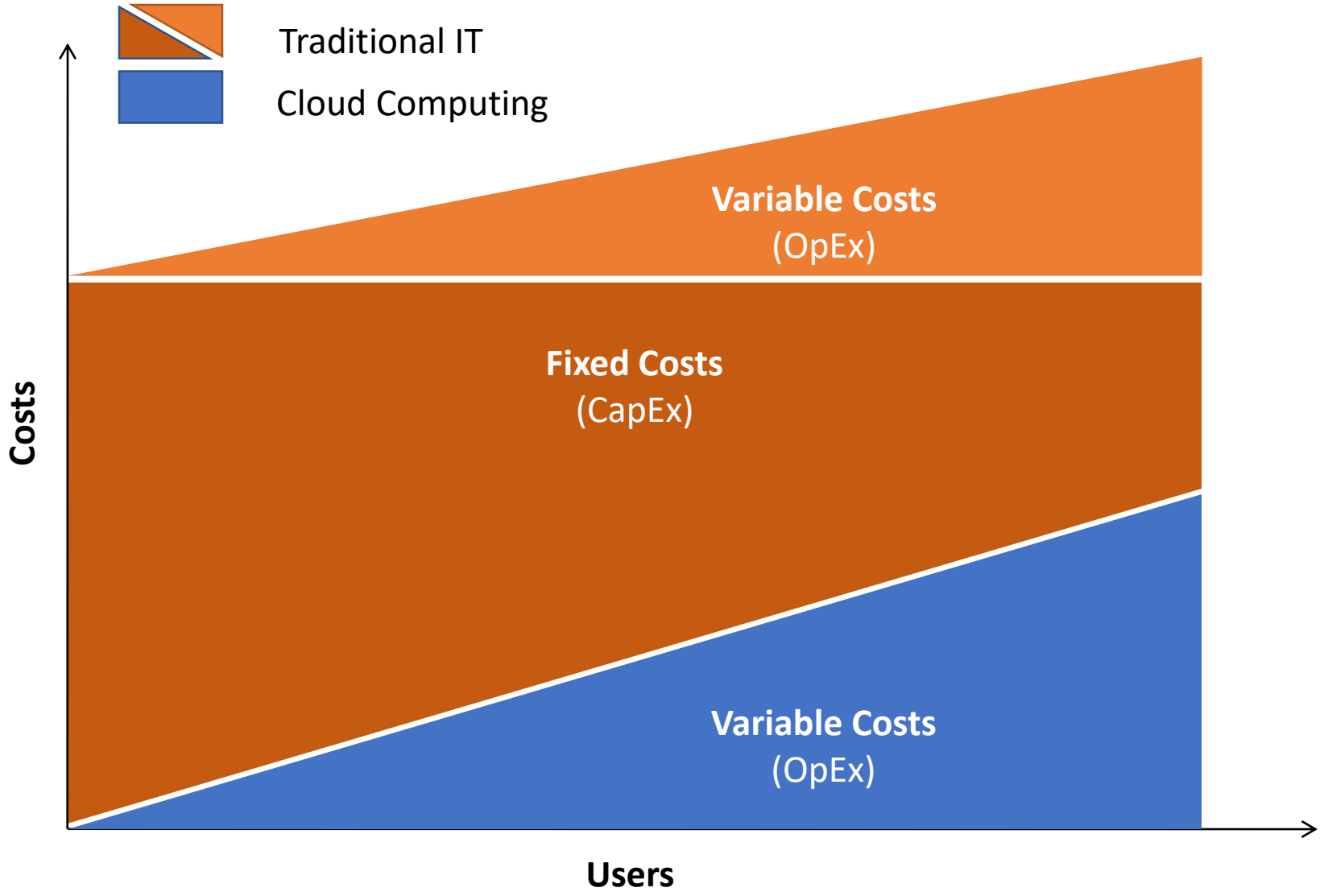
Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

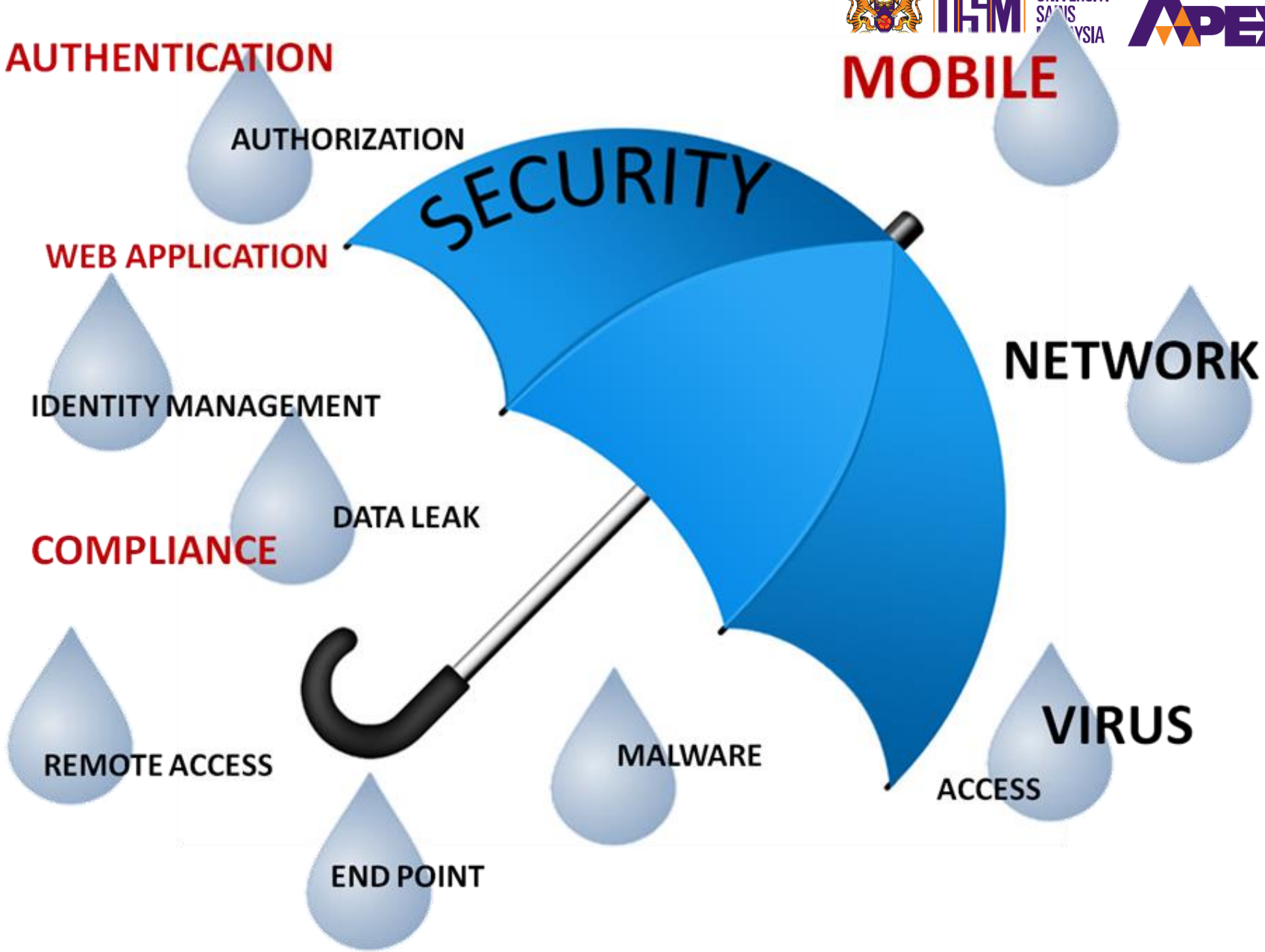

SaaS
Software as a Service
It's the model also referred as "on-demand software" in which an application is hosted as a service to customers who access it via the Internet. When the software is hosted off-site, the customer doesn't have to maintain it or support it.
PaaS
Platform as a Service
In the PaaS model, consumers purchase access to the platforms, enabling them to deploy their own software and applications on the cloud.
SaaS
Storage as a Service
It's a model in which a large service provider rents out space in their storage infrastructure to a smaller company or individual.
TaaS
Testing as a Service
Also called as "on-demand test environment" , It is a model in which software and its associated data are hosted centrally. In this the user can go for a on-demand test of the applications and softwares.
IaaS
Infrastructure as a Service
In this system, the consumer control and manage the system in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.
CaaS
Communication as a Service
Is an outsourced enterprise communications solution that can be leased from a single vendor.
THE CLOUD SERVICES UMBRELLA
MaaS
Management as a Service
Refers to enterprise monitoring. This service allows IT businesses and other businesses to remotely monitor and therefore manage networks, applications, services and more...
AaaS
Application as a Service
In this model, the user has the facility to enable the creation and hosting of APIs(application programming interfaces). It connects a locally-based application to a cloud-based storage system, so that a user can send data to it and access and work with data stored in it.
SECaaS
Security as a Service
In this model the large provider integrates their security services into a corporate infrastructure on a subscription basis.
NaaS
Network as a Service
is a business model for delivering network services virtually over the Internet on a pay-per-use or monthly subscription basis.
DaaS
Database as a Service
This model is similar to SaaS(Software as a Service) model. SaaS provides the softwares based on demand whereas the DaaS model provides the data on-demand regardless of the geographic or organizational separation of provider and consumer.
IDaaS
Identity as a Service
refers to the implementation of identity and access management (IAM) functionality, predominantly as web services, within a service-oriented architecture in an enterprise.
Reference Links:
http://abcdofcloud.wordpress.com/2013/05/03/xaas-anything-as-a-service/
http://www.techaaka.com/cloud-computing-services.html
Proudly Produced By : www.rishabhsoft.com
Twitter: twitter.com/RishabhSoft
Linkedin: linkedin.com/company/Rishabh-Software
Facebook: facebook.com/rishabhsoft
Rishabh Software
your reliable solution partner
IT, BPO, Engineering Services

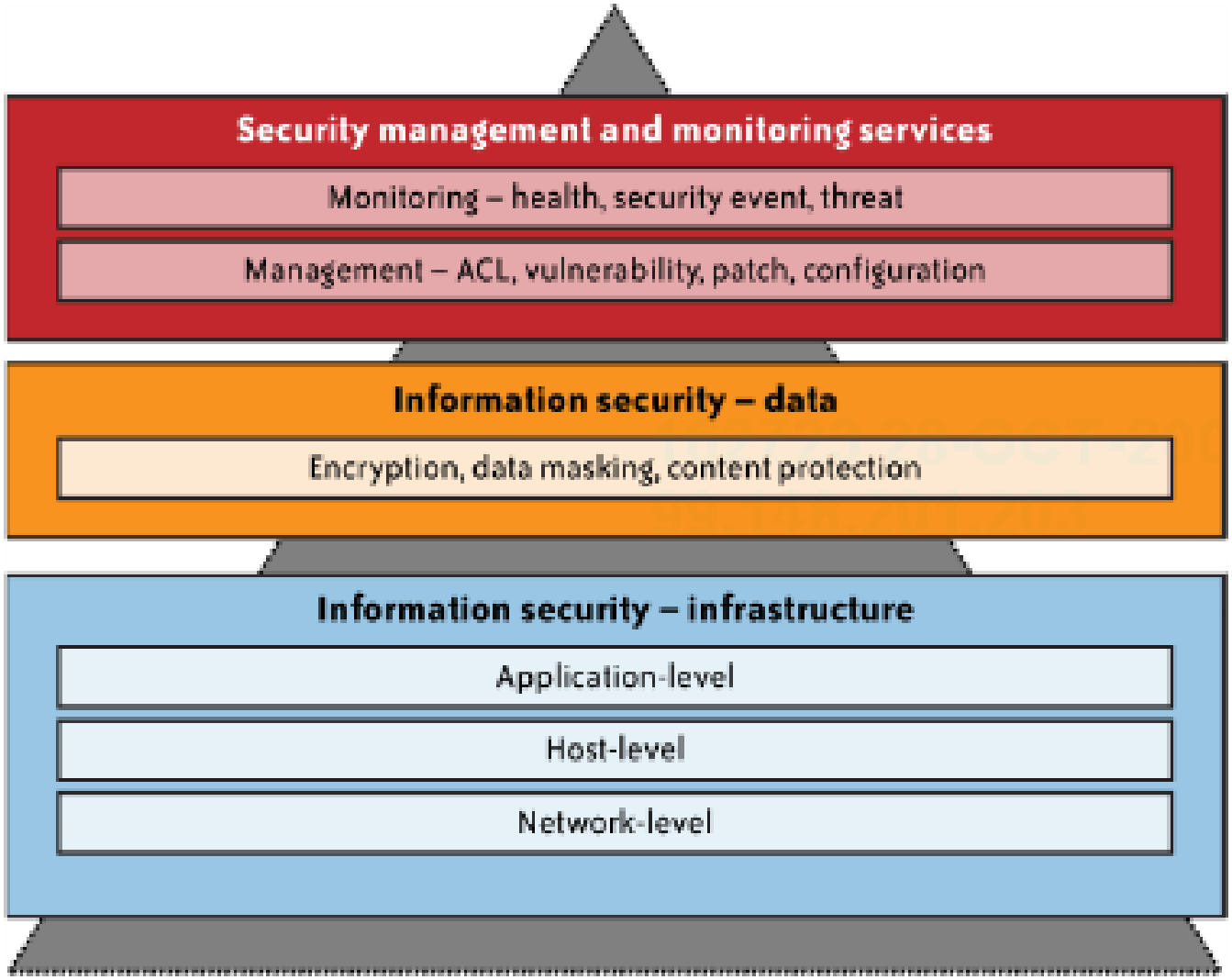
Cloud Computing Economics



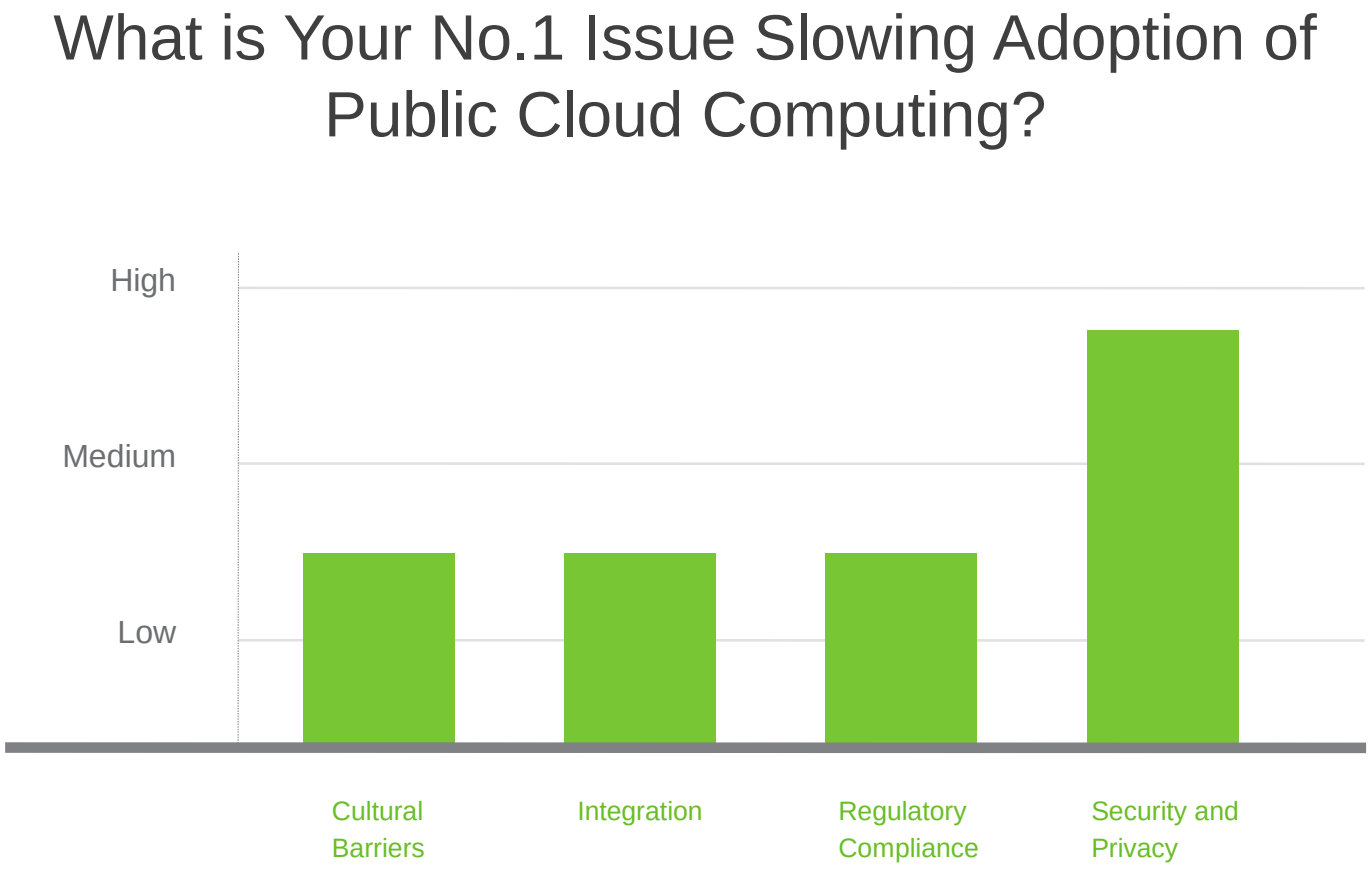
Pros and Cons

Cloud Computing Security


AUTHENTICATION
MOBILE
AUTHORIZATION
SECURITY
WEB APPLICATION
NETWORK
IDENTITY MANAGEMENT
DATA LEAK
COMPLIANCE
VIRUS
REMOTE ACCESS
MALWARE
ACCESS
END POINT


Security management and monitoring services
Monitoring – health, security event, threat
Management – ACL, vulnerability, patch, configuration
Information security – data
Encryption, data masking, content protection
Information security – infrastructure
Application-level
Host-level
Network-level

Cloud Security Statistics



Problems Associated with Cloud Computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Cloud Computing Privacy Issues

- Location and qualification of roles (controllers, processors - chain of (sub)providers and…affected individuals)
- Location and transborder flows (requirements)
- (Un) Certainty and (Mis) trust about the use of personal data (unlawful secondary use/ disclosure to LEAs ?)
- Concerns about security (security measures/ data breaches)
- Transparency

Lack of Trust in the Cloud

- A brief deviation from the talk
  - (But still related)
  - Trusting a third party requires taking risks
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed toward the same path?

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud
      - But can they be managed in some way by the consumer?
  - Lack of trust
    - Increase trust (mechanisms)
      - Technology
      - Policy, regulation
      - Contracts (incentives): topic of a future talk
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

The Notorious Nine Threats

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues
10. BYOC

Open Source Advantages

- Leverage the work of a growing community of developers
- Works across multiple hardware infrastructure
- Possible to deploy at service providers and on-premise
- Customized to fit individual needs or to add additional services

What is OpenStack

OpenStack is an open source cloud IaaS platform which provides compute, storage, and networking resources with service components.

OpenStack is open source software for creating private and public clouds, built and disseminated by a large and democratic community of developers, in collaboration with users.

OpenStack is managed by the OpenStack Foundation, a non-profit that oversees both development and community-building around the project.

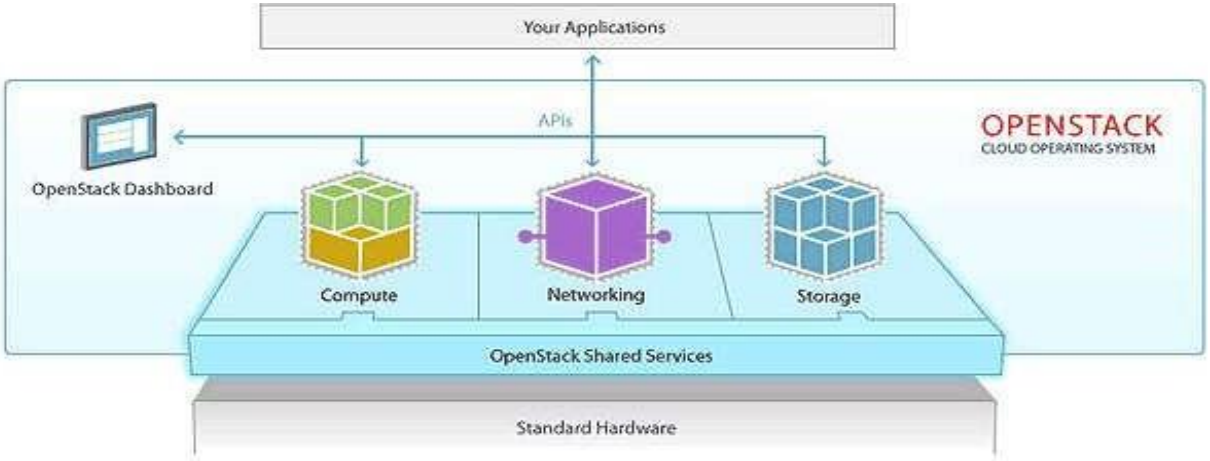
Introduction

OpenStack lets users deploy virtual machines and other instances that handle different tasks for managing a cloud environment on the fly.

It makes horizontal scaling easy, which means that tasks that benefit from running concurrently can easily serve more or fewer users on the fly by just spinning up more instances.

For example, a mobile application that needs to communicate with a remote server might be able to divide the work of communicating with each user across many different instances, all communicating with one another but scaling quickly and easily as the application gains more users.

OpenStack is open source software, which means that anyone who chooses to can access the source code, make any changes or modifications they need, and freely share these changes back out to the community at large. It also means that OpenStack has the benefit of thousands of developers all over the world working in tandem to develop the strongest, most robust, and most secure product that they can.



Major Components of OpenStack

Nova (Compute)

Swift (Object Storage)

Cinder (Block Storage)

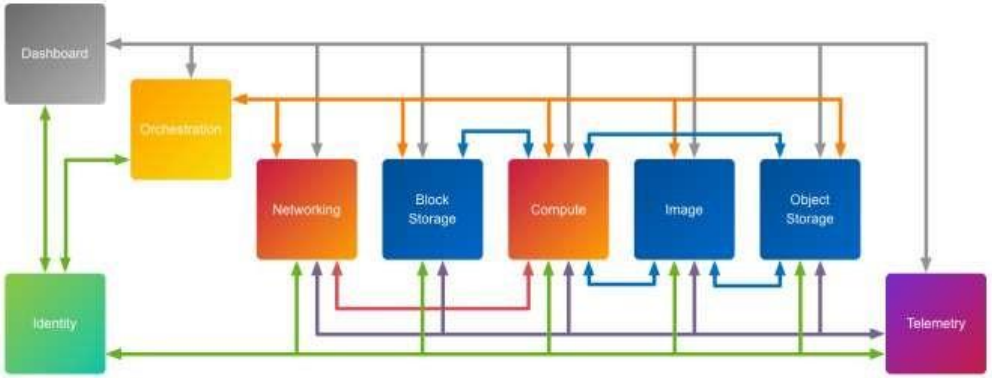
Glance (Image Service)

Neutron (Networking)

Horizon (Dashboard)

Ceilometer (Telemetry)

Heat (Orchestration)



Nova (Compute)

Nova compute or the king service provides a platform on which we are going to run our guest machines; It's the virtual machine provisioning and management module that defines drivers that interact with underlying virtualization. It provides a Control plane for an underlying hypervisors. Each hypervisor requires a separate Nova Instance. Nova supports almost all hypervisors known to man.

Glance (Image Service)

In simple words glance is the Image Registry, it stores and Manage our guest (VM) images, Disk Images, snap shots etc. It also contains prebuilt VM templates so that you can try it on the fly. Instances are booted from our glance image registry. User can create custom images and upload them to Glance later reuse. A feature of Glance is to store images remotely so to save local disk space.

Swift (Object Storage)

Swift Offers cloud storage software, Look at it as Dropbox or Google drive, as they are not attached to servers, they are individual addressable objects. It's built for scale and optimized for durability, availability, and concurrency across the entire data set. Swift is ideal for storing unstructured data that can grow without bound. Swift provides redundancy checksum for files, Files are stored as segments and a manifest file tracks them.

Ceilometer (Telemetry)

This module is responsible for metering Information. It can be used generate bills and based on the statistics of usage. Its API can be used with external billing systems.

Administrators can create certain alarms that are triggered based on performance statistics

Neutron (Networking)

Neutron, the networking component which was formally called Quantum. This component provides the software defined Networking Stack for Openstack. It Provides networking as a service. It gives the cloud tenants an API to build rich networking topologies, and configure advanced network policies in the cloud. It enables innovation plugins (open and closed source) that introduce advanced network capabilities which let anyone build advanced network services (open and closed source) that plug into Openstack tenant networks means that you can create advance managed switches and routers. You can even create an intelligent switch from a PC (Yes you can use it as a standalone component) and use it to replace your managed switch or at least make it act as a backup Switch.

Horizon (Dashboard)

Horizon is the Dashboard to Openstack, your eyes and ears. It provides a web based user interface to OpenStack services including Nova, Swift, Keystone etc.

Cinder (Block Storage)

Cinder is also one of the storage modules of Openstack; Think of it as an external hard drive or like a USB device. It has the performance characteristics of a Hard drive but much slower then Swift and has low latency. Block Volume are created in swift
and attached to running Volumes for which you want to attach an extra partition or for copying data to it. It survives the termination of an Instance. It is used to keep persistence storage. Cinder Images are mostly stored on our shared storage environment for readily availability. These Images can be clones and snapshot which can be turned in to bootable images. Its similar to Amazon Elastic block Storage.

Heat (Orchestration)

It creates a human and machine-accessible service for managing the entire lifecycle of infrastructure and applications within Openstack clouds. It contains human readable templates with simple instruction that is read by the Heat Engine. Heat along with ceilometer (explained below) can create an auto-scaling the cloud.

Why to use OpenStack?

- Enables rapid innovation
- Cuts down time-to-market
- Boosts scalability and resource utilization
- Eases regulatory compliance
- Devoid of vendor lock-in

Who is usingOpenStack?

List of top companies using OpenStack.

Company	Website	Country	Revenue	Company Size
Red Hat Inc	redhat.com	United States	>1000M	5000-10000
ViaSat, Inc.	viasat.com	United States	>1000M	1000-5000
World Wide Technology	wwt.com	United States	>1000M	1000-5000
Mirantis, Inc.	mirantis.com	United States	50M-100M	500-1000
Canonical Ltd.	canonical.com	United Kingdom	50M-100M	500-1000

Companies using OpenStack, by industry

Industry	Number of companies
Computer Software	1957
Information Technology and Services	1103
Staffing and Recruiting	449
Higher Education	286
Telecommunications	256
Computer Hardware	194
Internet	171
Hospital & Health Care	125
Financial Services	107
Retail	94

OpenStack Community – 60+ companies

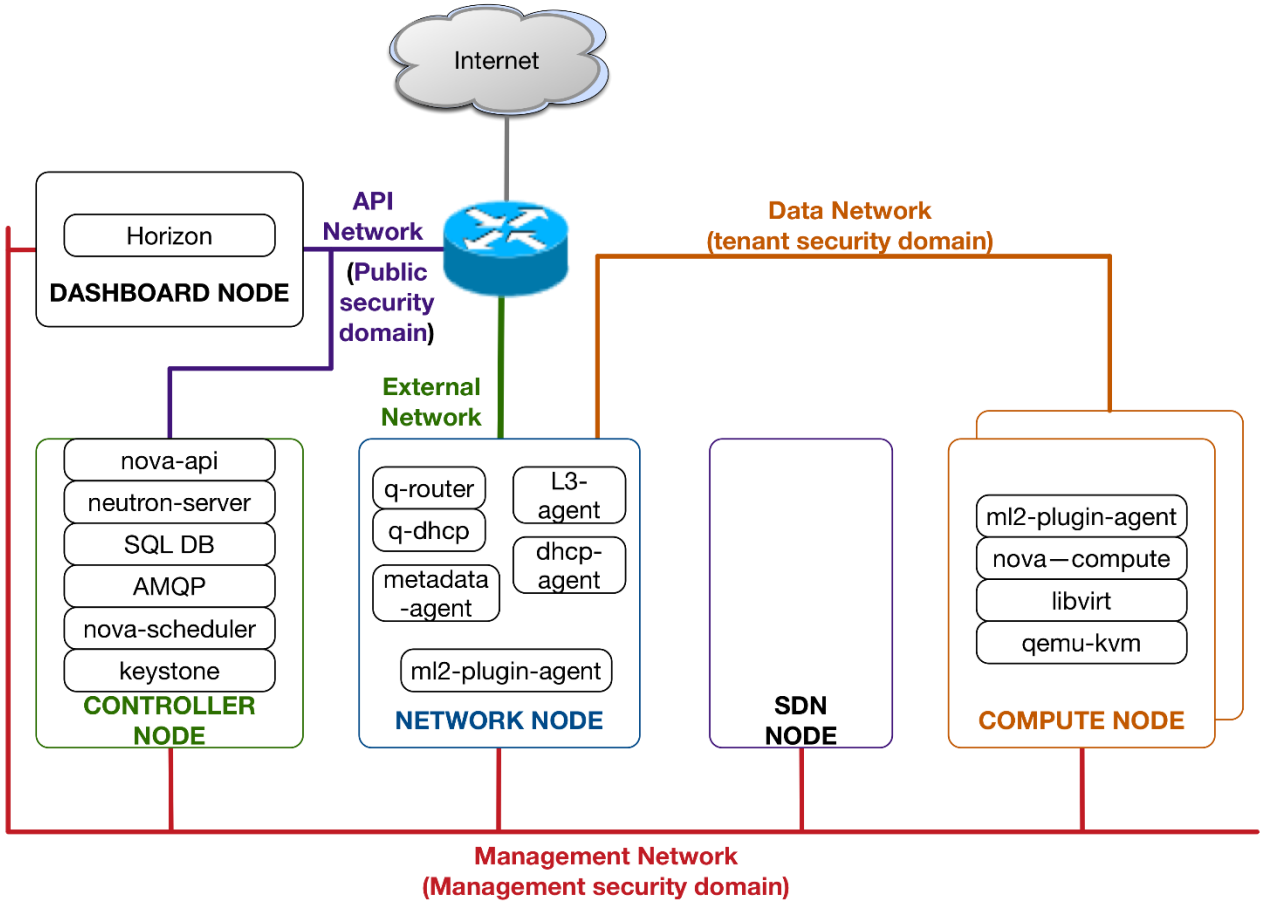
Review Security Strategies

- "Defense in depth" as the Primary Strategy
  - Use a series of defensive mechanisms
  - Protect each and every service component, communication channel and API access
  - Perimeter protection is one of the best defenses but not the only one
- Role Based Access Control (RBAC) & Domains
  - Restrict access to project resources based on Roles
  - Leverage Keystone "domains"
- Harden Neutron Service Components
  - Patch any reported neutron security vulnerabilities
    - e.g. https://www.cvedetails.com/vulnerability-list/vendor_id-11727/Openstack.html
  - Proper service configuration (Service owner, file permissions etc.)

Review Security Strategies (Continued..)

- Evaluate the security impact of using a tenant network type
  - Flat/VLAN/VXLAN/GRE etc.
- Limit Resources available to Projects
  - Self-Service network users have the ability to create, update, and destroy network resources
  - Set Quotas to limit network resources
- Isolate Network access
  - Security domains to control interaction to networking services
  - Network segmentation for various types of traffic (e.g. Management, API, External, Data)
  - Use Neutron Security Groups & Anti-Spoofing filters to protect project instances

Network Security Domains



Networking Security Checklist

- Are all interactions with the networking service isolated into security domains?
- Does the ML2 mechanism driver mitigate ARP spoofing?
- Considered the pros and cons of supporting various tenant network types?
- Have you hardened all neutron service components?
- Are you using neutron security-groups and enabled port-security?
- Are all communications using SSL encryption?
- Has RBAC been implemented using the concept of least privilege?
- Have you investigated the maturity and security features of the various pluggable neutron components you are using?
- Are you using quotas to limit project resources?

First International Conference on

Advances in Cybersecurity

aces.usm.my

aces@usm.my

Thank You

Assoc. Prof. Dr. Selvakumar Manickam

selva@usm.my

selvadt@gmail.com