Cloud Architecture and Management

M.I. Deen

General Manager (Enterprise Solutions)

Sri Lanka Telecom

akaza

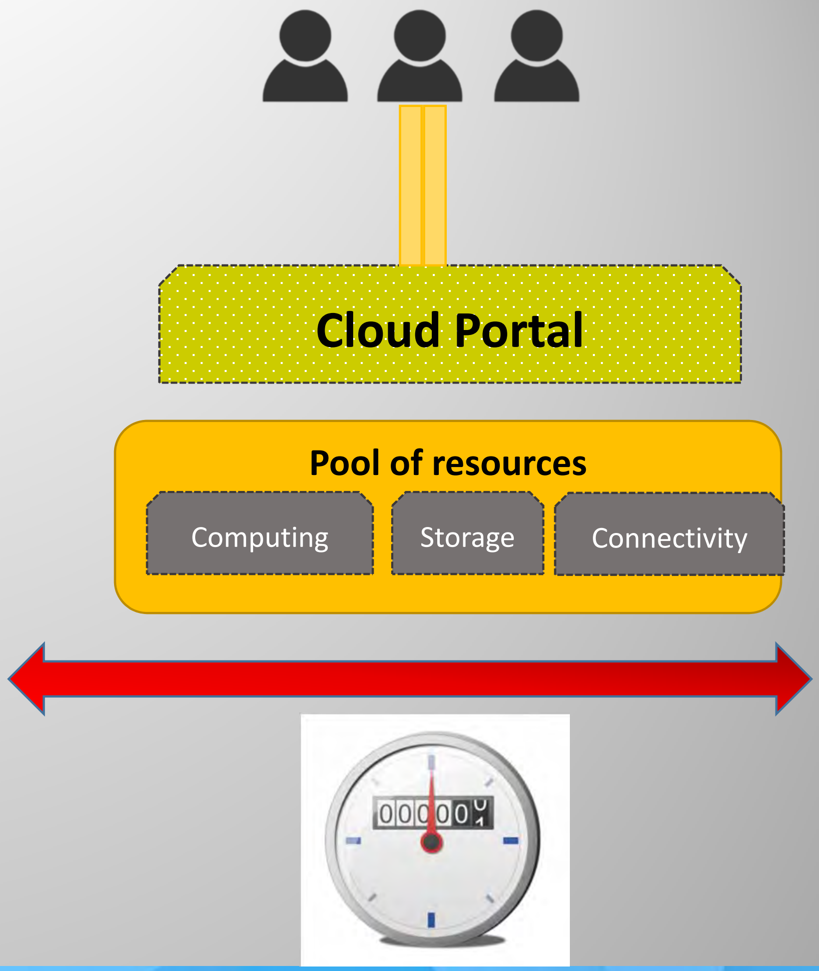
🟦	**Cloud Computing Architecture** - Reference Architecture, Terminology and Definitions - Akaza Cloud Architecture - Feature/Aspects of the cloud architecture
🟨	**Cloud Computing Portability** - Key considerations for cloud portability - Use case : App Life Cycle Management
🟩	**Cloud Computing Interoperability** - Key considerations for cloud interoperability - Use Case : Integration with Enterprise Private cloud and SP Private cloud
🟥	**Security and Compliance** - Security and Compliance from CSP and customer perspective - Physical implementation of security between enterprise and cloud - Some common compliance standards
🟪	**Telco Cloud vision** - Where Enterprise Cloud meets Telco Cloud

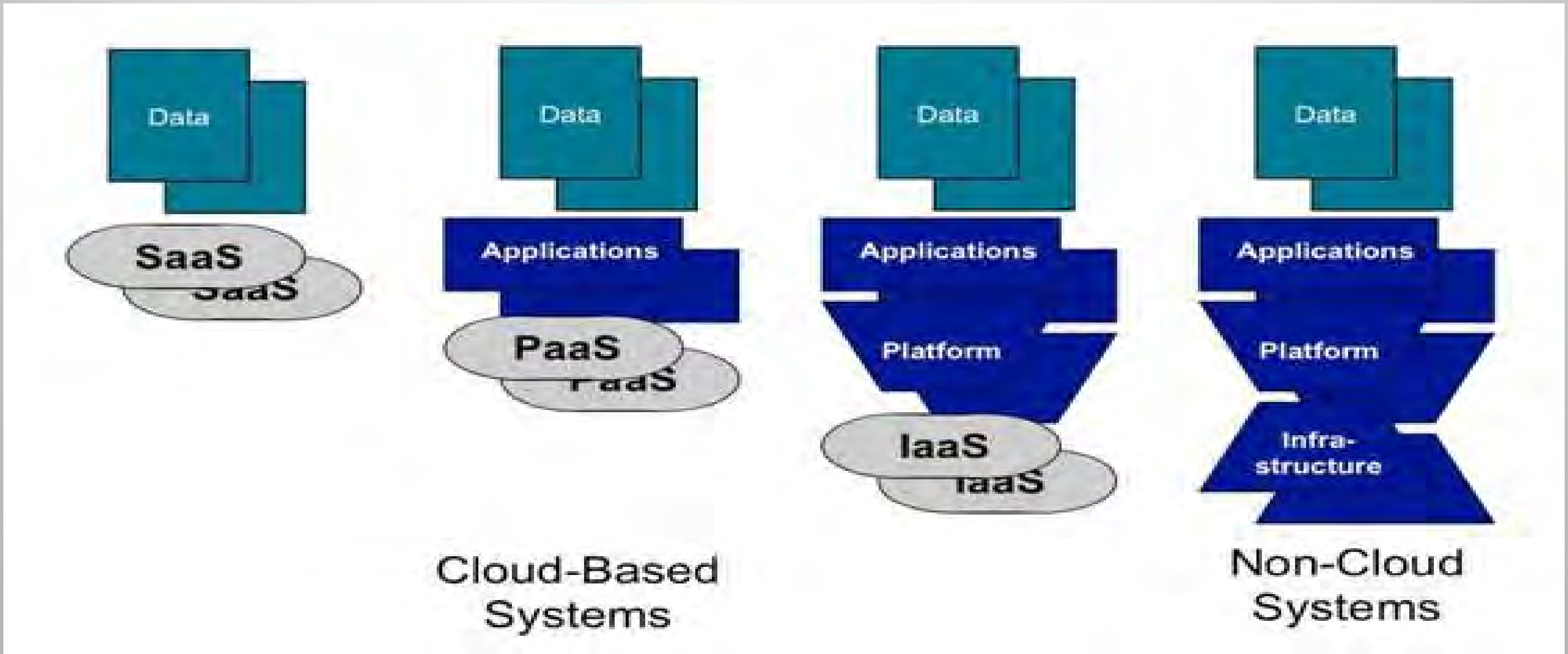
Cloud Computing Architecture

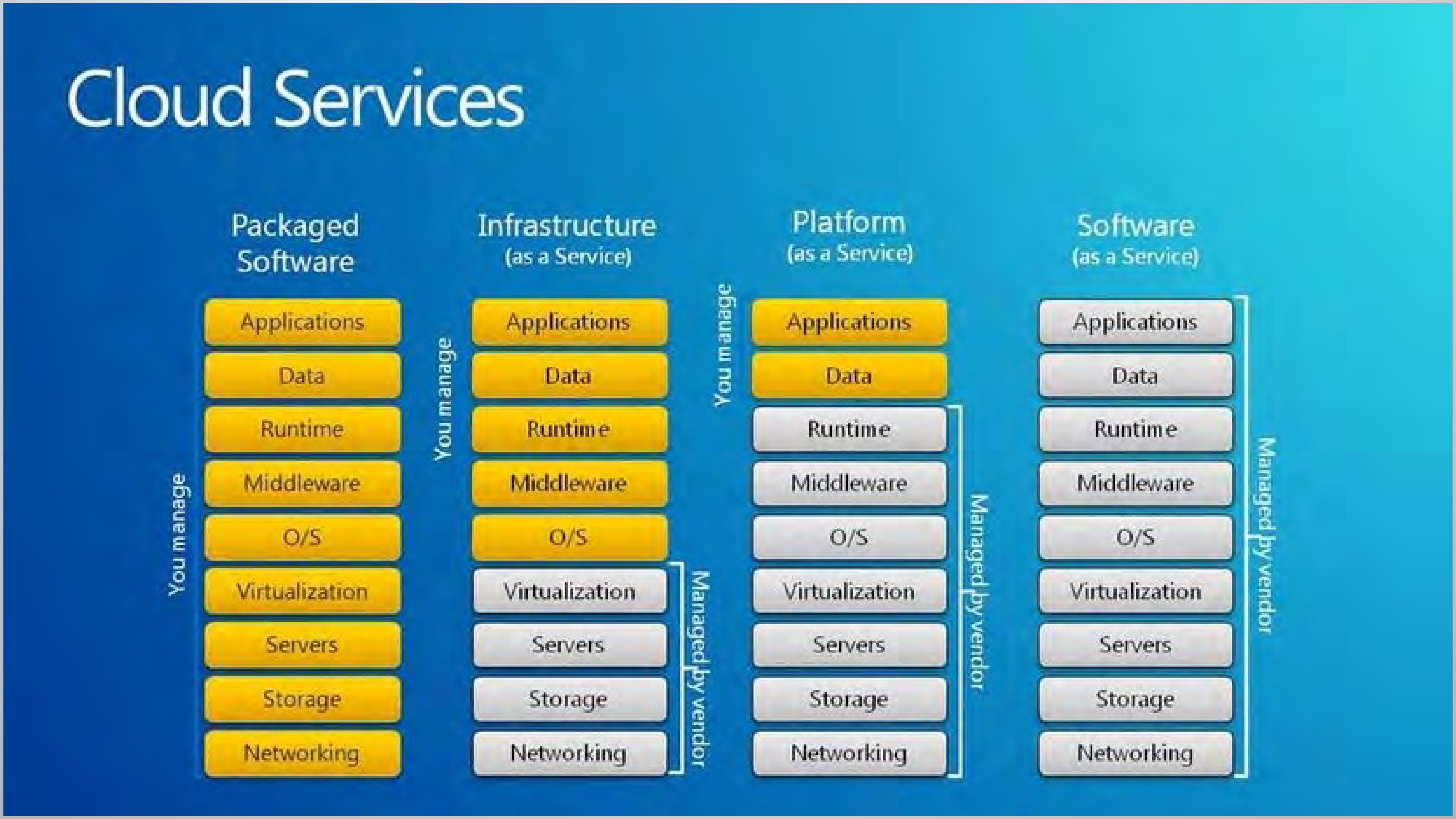
akaza

Basic Tenets of a Cloud Computing Architecture

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service




Data
SaaS
SaaS
Data
Applications
PaaS
PaaS
Data
Applications
Platform
IaaS
IaaS
Data
Applications
Platform
Infra-
structure
Cloud-Based
Systems
Non-Cloud
Systems



Cloud Services

Packaged Software	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud Computing Reference Architecture

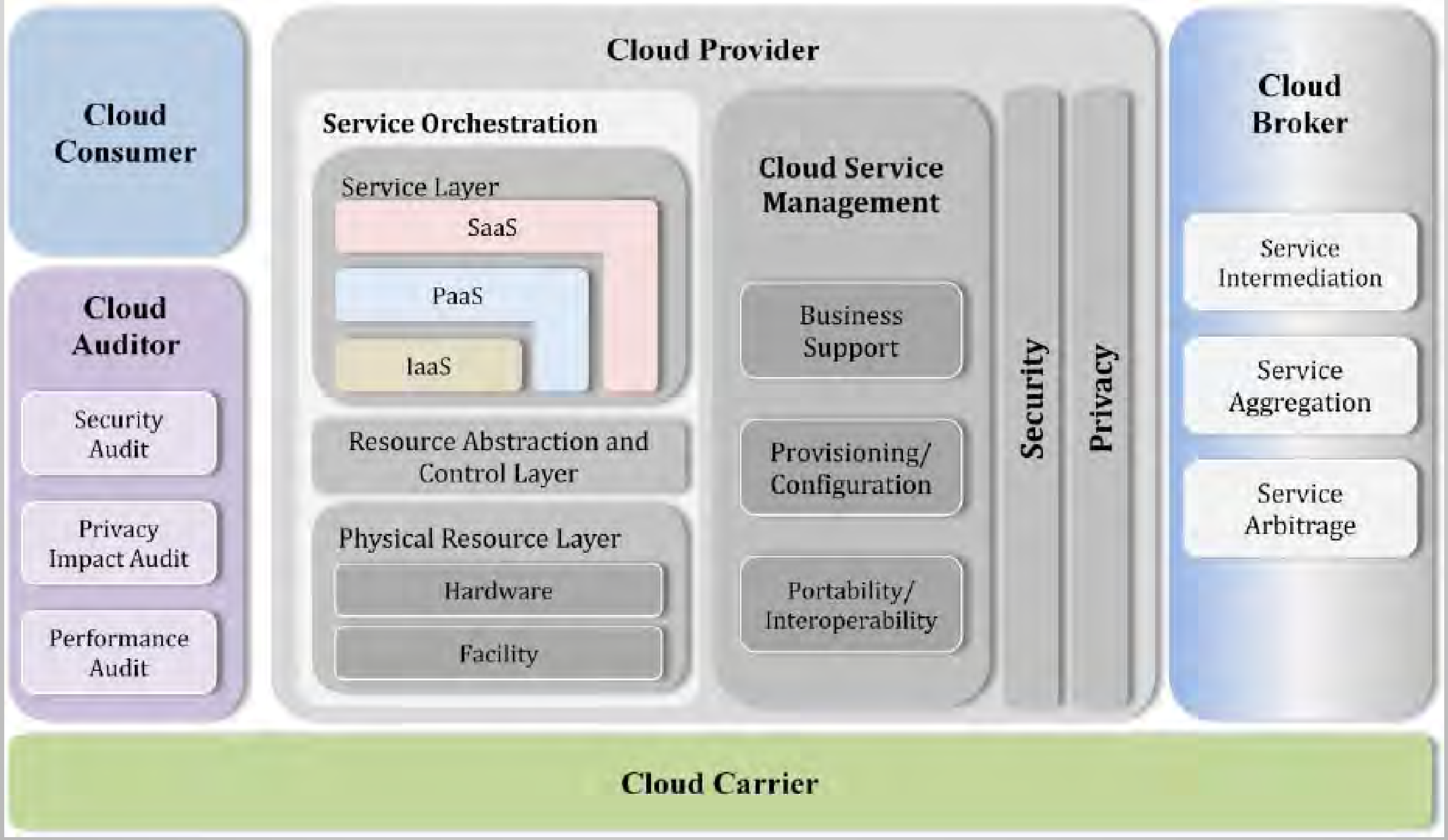


Figure 1: NIST The Conceptual Reference Model

	Terminology of the Reference Architecture (NIST Refernece Model)
Cloud Service Auditor	(1) A party that can conduct independent examination of Cloud Service controls with the intent to express an opinion thereon. (2) Audits are performed to verify conformance to standards through review of objective evidence.
Cloud Service Broker	(1) An entity that manages the use, performance, and delivery of Cloud Services, and negotiates relationships between Cloud Service Providers and Cloud Service Consumers. (2) Key capabilities provided by Cloud Service Brokers are: Cloud Service on-boarding, Cloud readiness assessment, Application and data migration, Cloud Service Provider capabilities evaluation
Cloud Service Consumer	(1) An entity as the principal stakeholder that maintains a business relationship with, and uses the service from, a Cloud Service Provider.
Cloud Service Developer	(1) An entity that develops the technical as well as the business aspects of a Cloud Service offering, which may be part of the organization of the Cloud Service Consumer or Cloud Service Provider. (2) A Cloud Service Developer leverages the development and operational tools to develop and compose a service or set of services.
Cloud Service Provider	An entity which is responsible for making a Cloud Service available to interested parties.

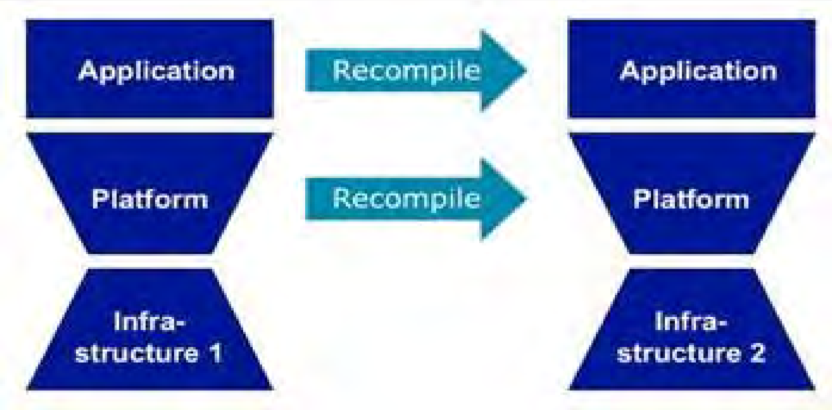
	Salient Aspects of the Akaza Cloud Architecture
	Self Contained Architecture leveraging on Citrix Cloudstack and Cloud Portal Business Manager
	Total Cloud Service Lifecycle Management from Lead Management -> Product/Order Management -> Resource Management -> Showback/Chargeback -> Billing Integration
	REST based API allowing Service Integration (including integration and portability to AWS) PaaS – Cumulogic AppaaS/SaaS – Appcara DaaS – Xen Desktop (Shared/Dedicated)
	Service Aggregation through the Cloud Portal
	Channel Management for Reseller enablement
	Extensible to conformance of Security/Firewall control and Compliance
	Different availability Zones for different categories/characteristics (eg. Product category)

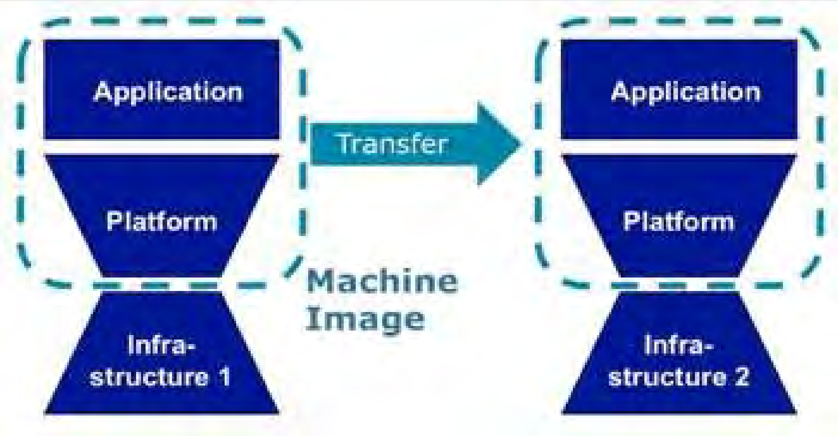
Cloud Computing Portability

Key consideration for cloud computing portability categories

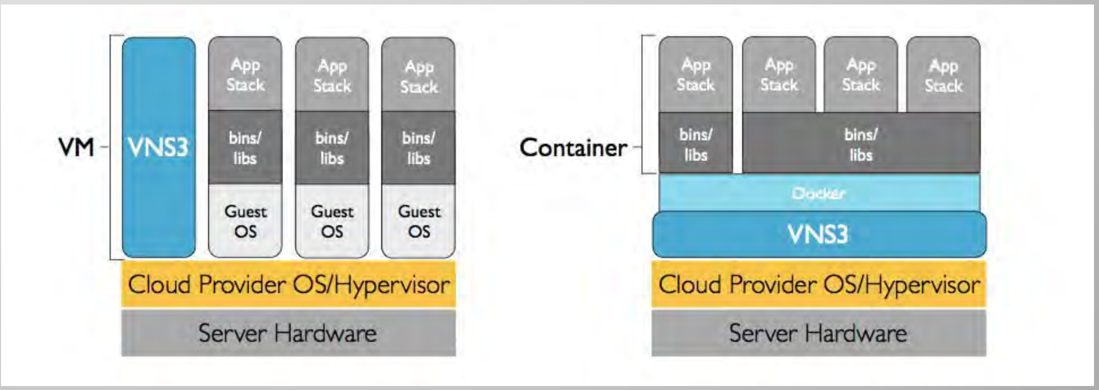
Category	Description	Challenges/Considerations
Data Portability	(1) Enables re-use of data components across different applications. (2) Degree of ease in porting data and environment when changing SaaS vendors. (3) SLA and commercial arrangements is the focus.	
Application Portability	(1) Application portability enables the re-use of application components across cloud PaaS services and traditional computing platforms	(1) Moving the Enterprise App from one PaaS provider to a different PaaS provider for cost/performance reasons. (2) Application and Platform adhere to standard interface
Platform Portability	(1) Re-use of platform components across cloud IaaS services and non-cloud infrastructure – *platform source portability* (2) Re-use of bundles containing applications and data with their supporting platforms – *machine image portability*	

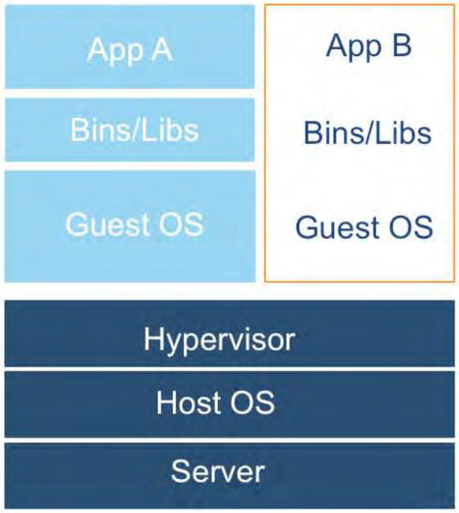
Graphical Depiction of Cloud Computing Portability





Docker is a very nicely constructed container architecture that provides better cloud-to-cloud portability and workload management. It also sets a great foundation to build cloud-based distributed systems that can be moved around much easier than the cloud workloads we manage these days

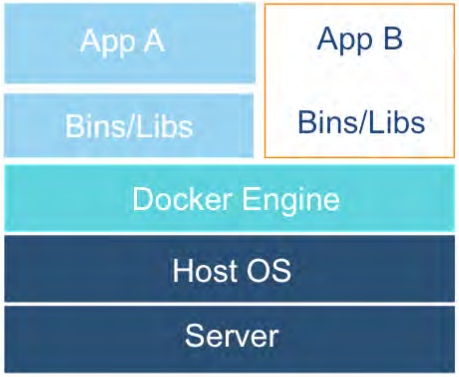




App A
Bins/Libs
Guest OS
App B
Bins/Libs
Guest OS
Hypervisor
Host OS
Server

Virtual Machines

Each virtualized application includes not only the application - which may be only 10s of MB- and the necessary binaries and libraries, but also an entire guest operating system - which may weigh 10s of GB.

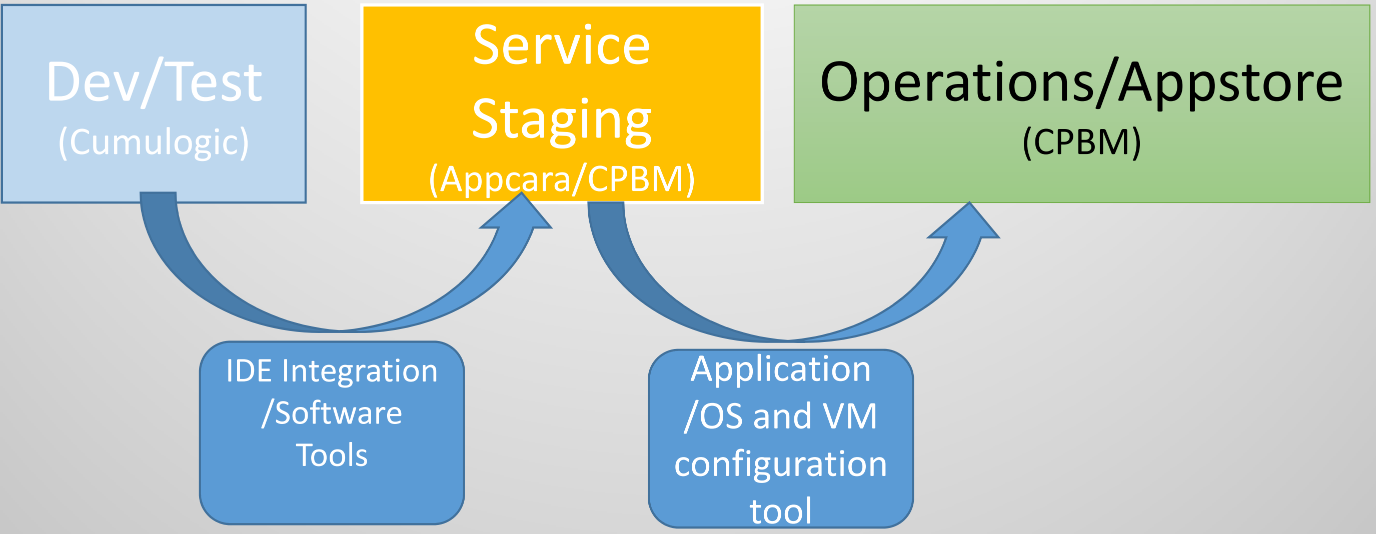


App A
Bins/Libs
App B
Bins/Libs
Docker Engine
Host OS
Server

Docker

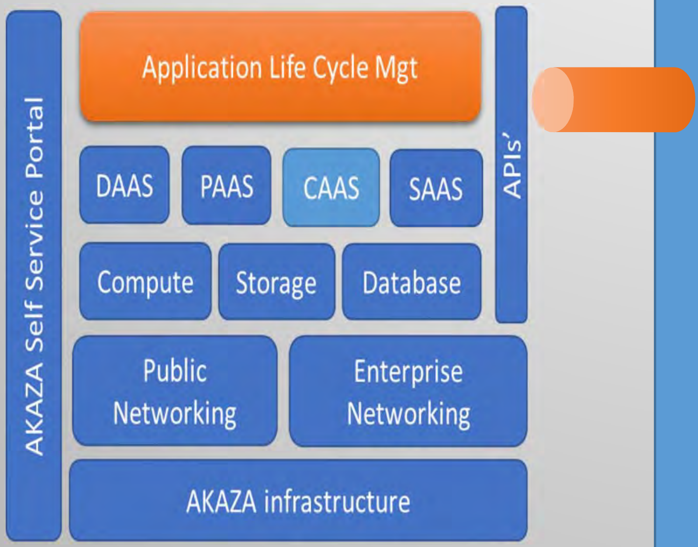
The Docker Engine container comprises just the application and its dependencies. It runs as an isolated process in userspace on the host operating system, sharing the kernel with other containers. Thus, it enjoys the resource isolation and allocation benefits of VMs but is much more portable and efficient.

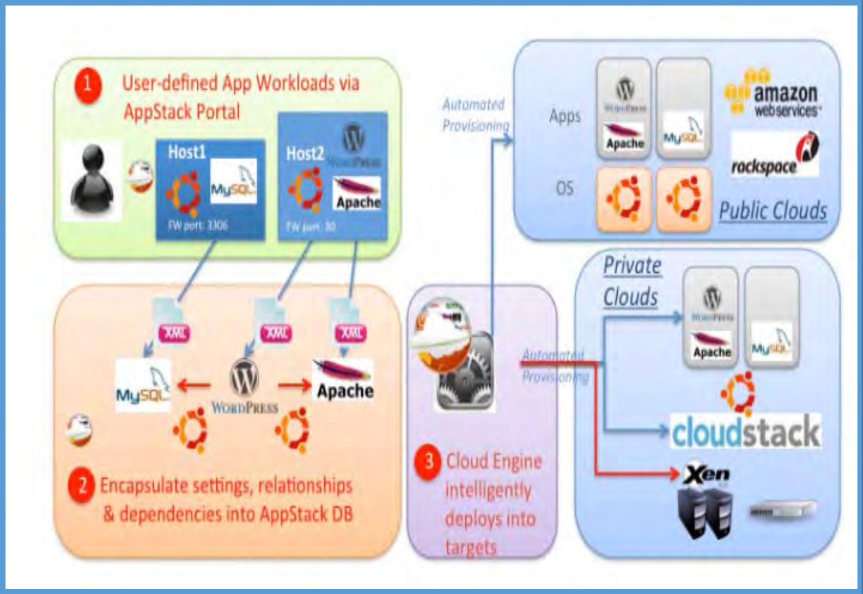
Akaza : Towards Applications/IT Life Cycle Management



Support Dev/Test/Ops environment for Application lifecycle on the cloud
Software onboarding assurance though rule based scripts
Software version management
Ability to integrate to other private and public clouds

Cloud management Interface –Manage Application Life cycle Via Cloud





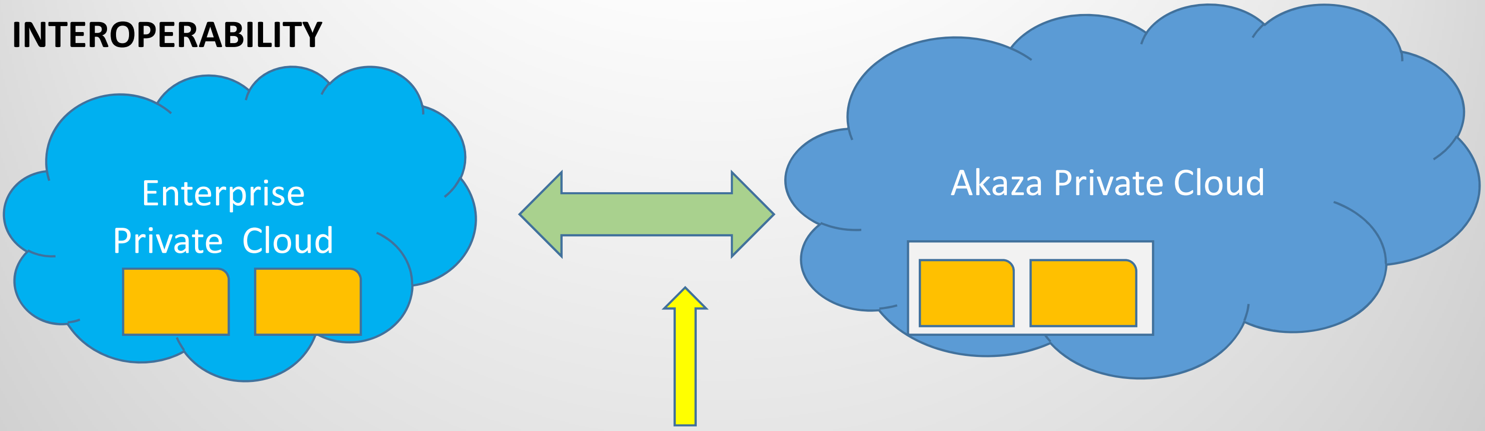
Cloud Computing Interoperability

akaza

Key consideration for cloud computing interoperability categories

Category	Description
Application Interoperability	(1) Interoperability between application components – - Deployed as SaaS - As Applications using PaaS, - As Applications on platforms using IaaS in a traditional enterprise IT environment, or on client devices. (2) An application component may be a complete monolithic application, or a part of a distributed application.
Platform Interoperability	Interoperability between platform components, which may be deployed - As PaaS - As Platforms on IaaS, in a traditional enterprise IT environment, or on client devices.
Management Interoperability	Interoperability between cloud services (SaaS, PaaS, or IaaS) and programs concerned with the implementation of on-demand self-service.
Public & Software Acquisition Interoperability	Interoperability between platforms, which includes PaaS services, App Stores and App Marketplace. Standard interfaces to these stores would lower the cost of cloud computing for software providers and users.

USE CASE ON INTEROPERABILITY



Private IP-VPN between clouds

Features :
Interoperability at the software integration level between software Components in multiple clouds using REST API
Unified view of VMWare (Enterprise) and Xen Hypevisor workloads on the Citrix Cloudplatform
http accessibilty Enterprise customer to Cloudportal/Appstore on a Private Web interface

Security and Compliance

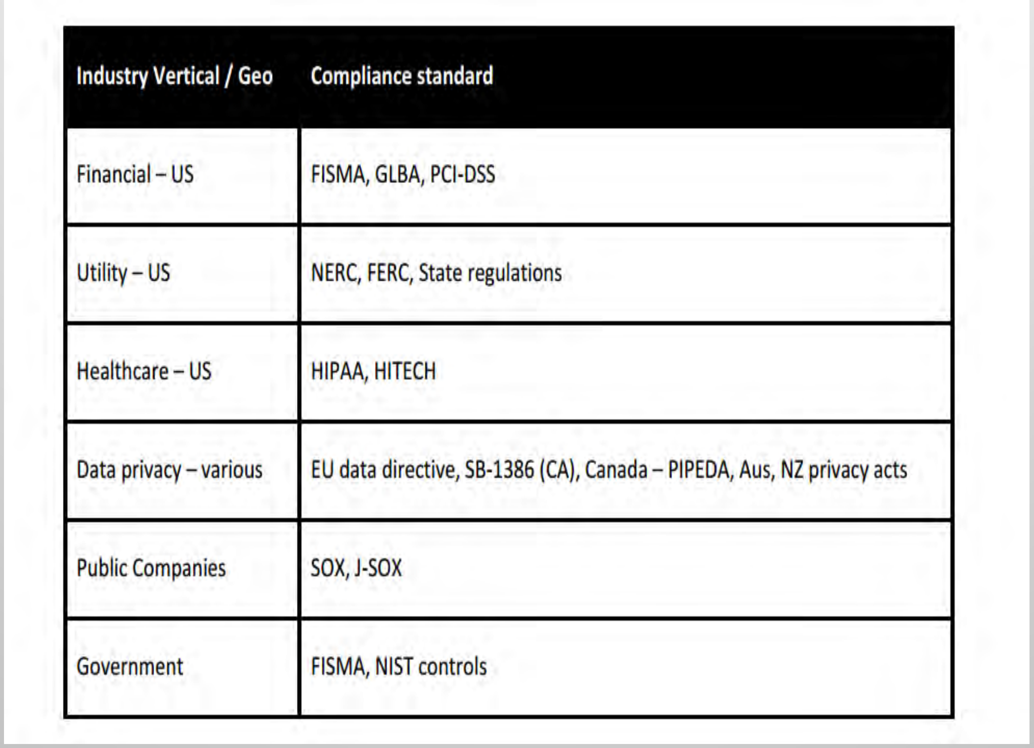
	Security	Governance/Risk/Compliance
Cloud Service Provider		
Cloud Assets/Infrastructure	-Install dedicated security team -Deploy VA in a proactive manner -Delieanate Management traffic to Workload traffic -Install log management and event correlation management -Firewalled VM Images -Security between tenancy and zone separation as firewall segments -Deploy Global IDS/IPS and WAF (for internal management system) - Automate Everything - Managed Security As A Service	- Security Policy Document - Best Practices and Guidance from Cloud Security Alliance - Adoption of standards such as ISMS, ISO 27002 - For Application Specific Hosting and Geo-based hosting adopt relevant standards such as ecommerce PCI-DSS and Healthcare HIPAA

Initial Risk Assessment as articulated by Cloud Security Alliance for Cloud Customers

Point of Address	Impact addressed
Identify the Assets for the Cloud Deployment	- Data - Application/Function/Processes
Evaluate the Asset	How important is the (Asset) data/function to the organization
Map the Asset to a potential cloud deployment model	The impact analysis in moving the asset/function etc. to the cloud eg. Public cloud
Evaluate potential cloud service model and providers	Degree of control at CSP tier and risk assessment of providers
Map out the potential data flow	Map out the data flow between organization, cloud and other nodes

Depending on the potential risk level in the deployment organizations could adhere
To guidance in 14 Domain Areas in security given by CSA.
See https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

Some of the common compliance standards



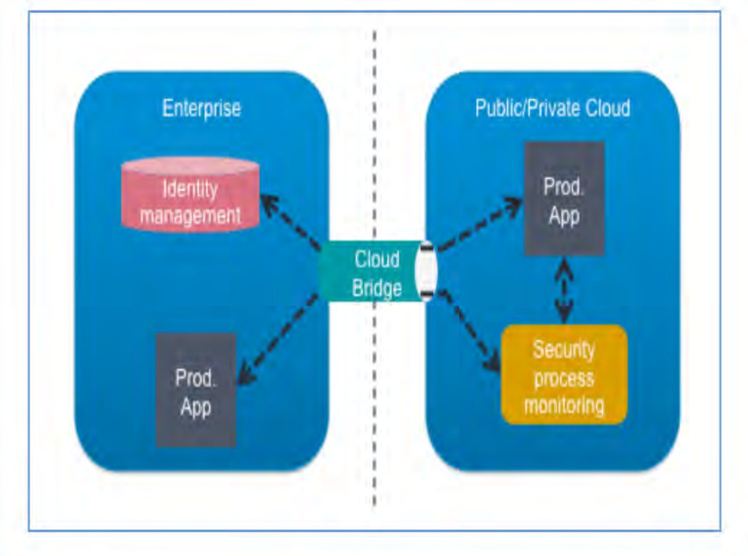
Industry Vertical / Geo	Compliance standard
Financial – US	FISMA, GLBA, PCI-DSS
Utility – US	NERC, FERC, State regulations
Healthcare – US	HIPAA, HITECH
Data privacy – various	EU data directive, SB-1386 (CA), Canada – PIPEDA, Aus, NZ privacy acts
Public Companies	SOX, J-SOX
Government	FISMA, NIST controls

A secure bridge and access between cloud and enterprise data center

- A secure bridge needs to be maintained between the cloud data center and the enterprise.

- This provides seamless, secure connectivity and enables certain security services (e.g., compliance reporting) running in the cloud to be used with applications running within the enterprise datacenter.

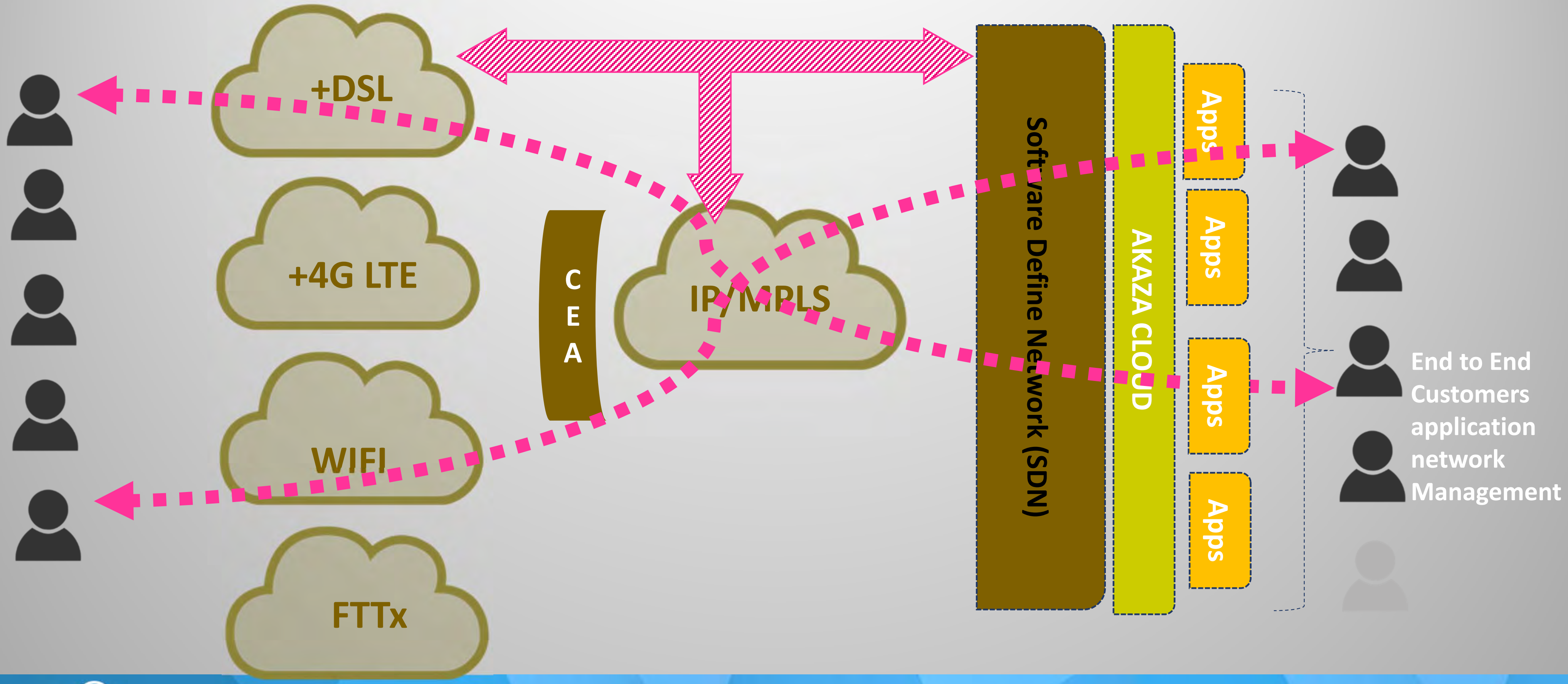
- This also allows the identity management infrastructure (e.g., directory services) running in the enterprise to be leveraged by applications running in the cloud.



Cloud Computing Interoperability

akaza

AKAZA Extension to the cloud Network -Akaza SDN



akaza

Thank You