Cloud Environments in a Nutshell

Developed By **Karen Baez**

Copyright CyberAdeptness LLC

HOW DOES IT WORK

A Cloud Environment is made possible by Virtualization Technology aka Hypervisor.

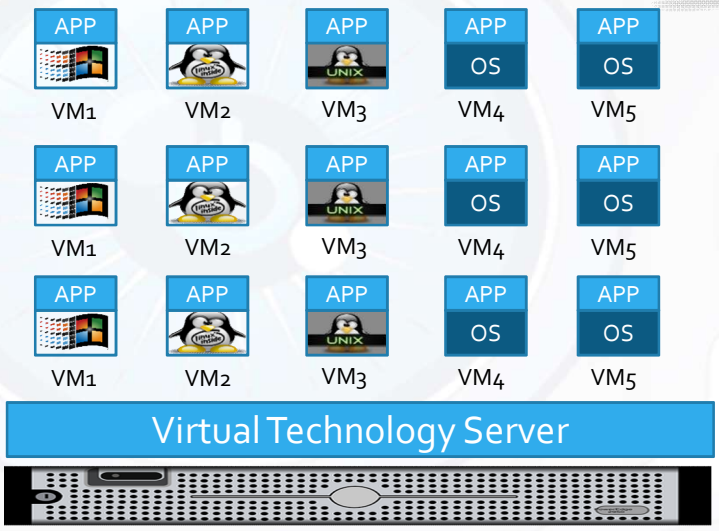
While the technology itself has been around and evolving for almost 50 years, the explosion of cloud services was initiated by VMware and it is still one of the top vendors in the area of virtualization.

The hypervisor allows an organization to shrink the number of physical servers it has to purchase to 2 or 4, each configured to handle 15+ virtual servers within.

Typical Datacenter

20 Physical Servers

Virtualized Datacenter



1 Physical Server, Hypervisor Technology, 15+ virtual servers

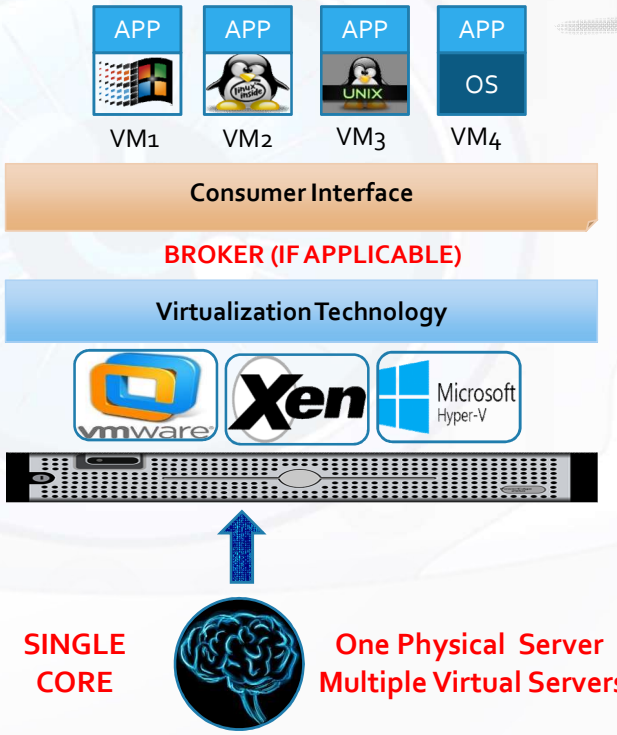
NOTE: The hardware configurations will determine the number of servers to be handled . A single powerful server can cost up to 15k new.

Copyright CyberAdeptness LLC

WHAT IS SERVER VIRTUALIZATION

Server Virtualization

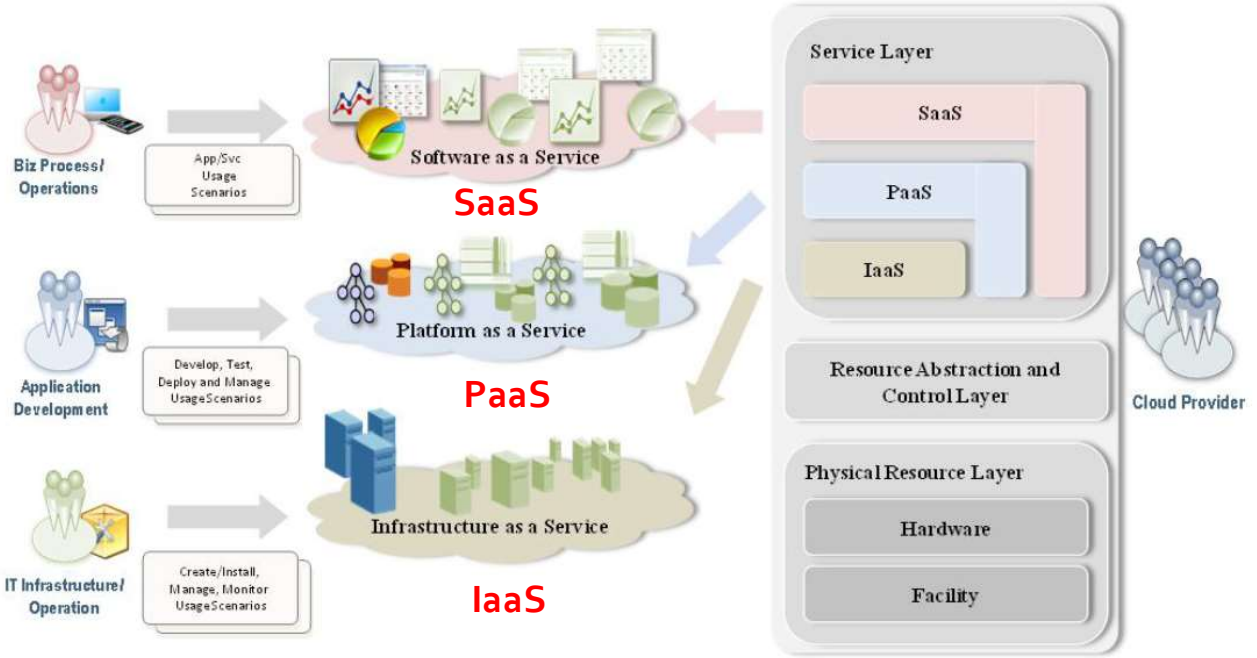
- Is the Core Method for Cloud Computing
- Server Consolidation is made possible by limiting the needs of physical servers to what matters. (Typically 8 to include Fail-Over and physical segmentation of environments)
- Hardware Resource Utilization will be 70-80% use vs. the typical 10-15% used by a single server.
- Physical and Geographical Limitations Non-existent
- Disaster Recovery is easier as failover can be applied.
- Deployment boundaries are limitless.
- Energy Savings are higher, those leading to lower capital expenses.



Copyright CyberAdeptness LLC

WHAT'S ARE THE TOP SERVICES

The Services are based on three unique models: IaaS, PaaS, and SaaS.



Copyright CyberAdeptness LLC

Cloud Actors

At a Glance

Copyright CyberAdeptness LLC

Who are the main Actors

As defined on the NIST cloud computing reference architecture, there are five (5) actors and they are:

Cloud Carrier

The intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers

Cloud Provider

Person, organization, or entity responsible for making a service available to Cloud Consumers.

Cloud Broker

An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud Auditor

A party that can conduct independent assessment of Cloud services, information system operations, performance and security of the cloud implementation

Cloud Consumer

Person or organization that maintains a business relationship with, and uses service from Cloud Providers.

NOTE: Cloud environments can have up to 4 unique actors, which means security is spread among each individual entity responsible for the underlying components.

Copyright CyberAdeptness LLC

Cloud Deployments

At a Glance

Copyright CyberAdeptness LLC

HOW MANY DEPLOYMENTS EXIST

Currently, there are four (4) deployment models, each with their own unique security risks. They are:

The next few slides will provide a visual a brief description and visual for each model.

Copyright CyberAdeptness LLC

Private Cloud

Copyright CyberAdeptness LLC

Private Cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

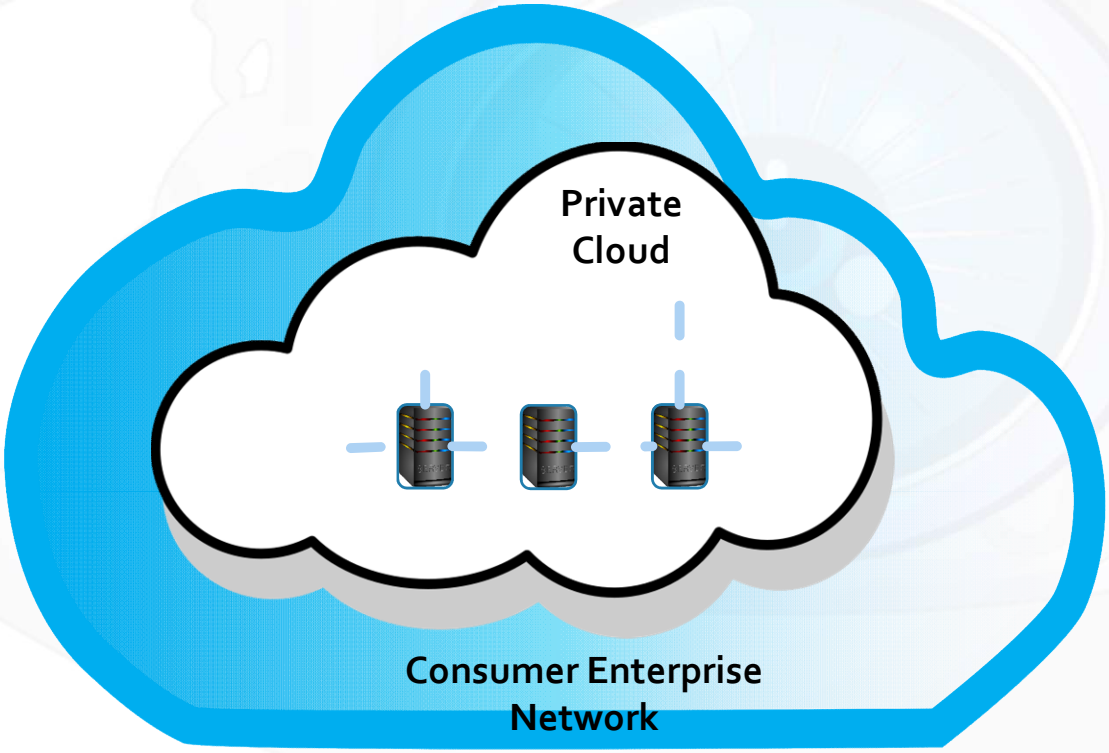
Most private clouds are develop within the organizations internal enterprise network or private cloud offerings from a cloud providers (typically extending the internal network into a service providers hosting center).

Best OPTION when DATA Security is a Concern and such is impacted by multiple- standards.

In this case, the organization manages the infrastructure and is the SOLE Consumer, those having the flexibility to apply security with any standards impacting the organization and it's consumers.

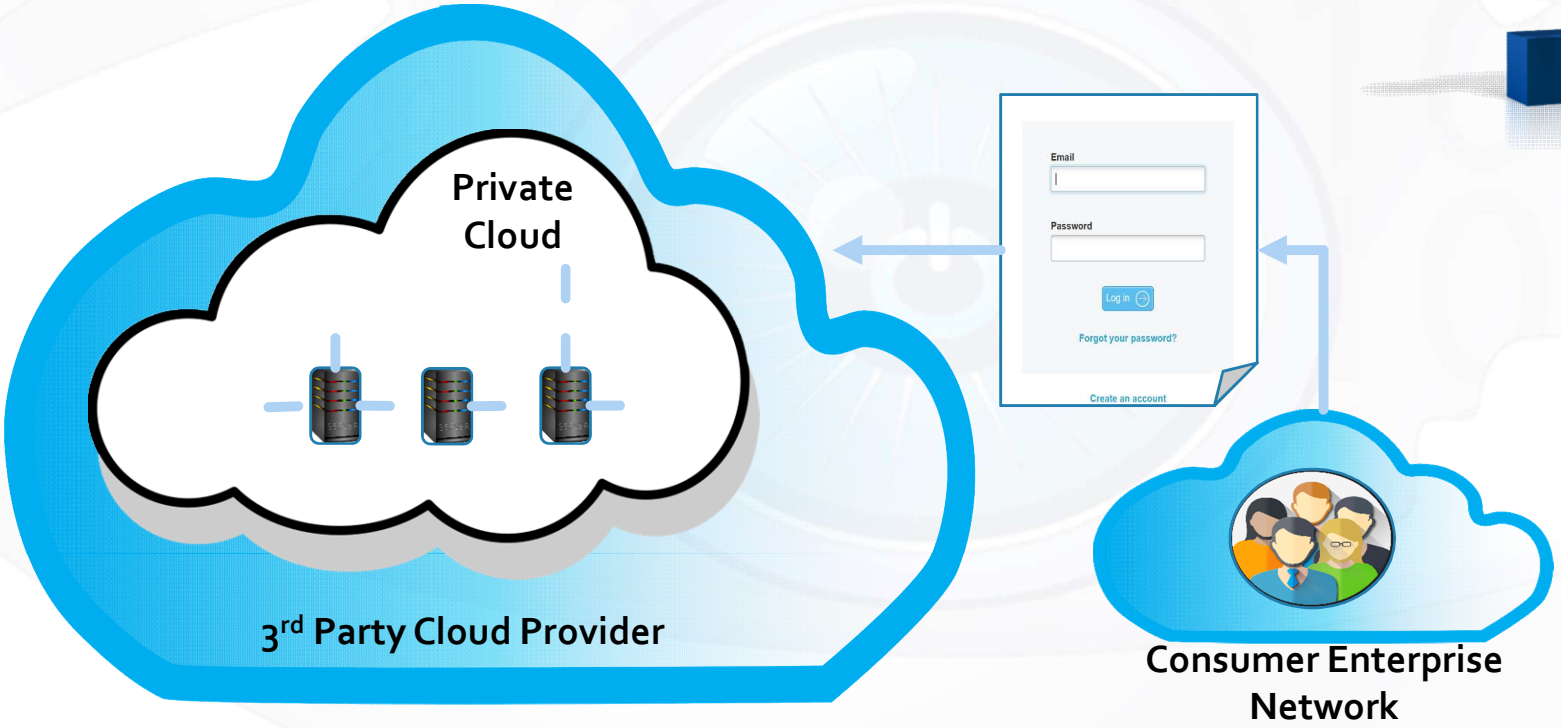
Copyright CyberAdeptness LLC

PRIVATE CLOUD - ON-SITE



Copyright CyberAdeptness LLC

PRIVATE CLOUD - OFFSITE



Community Cloud

Copyright CyberAdeptness LLC

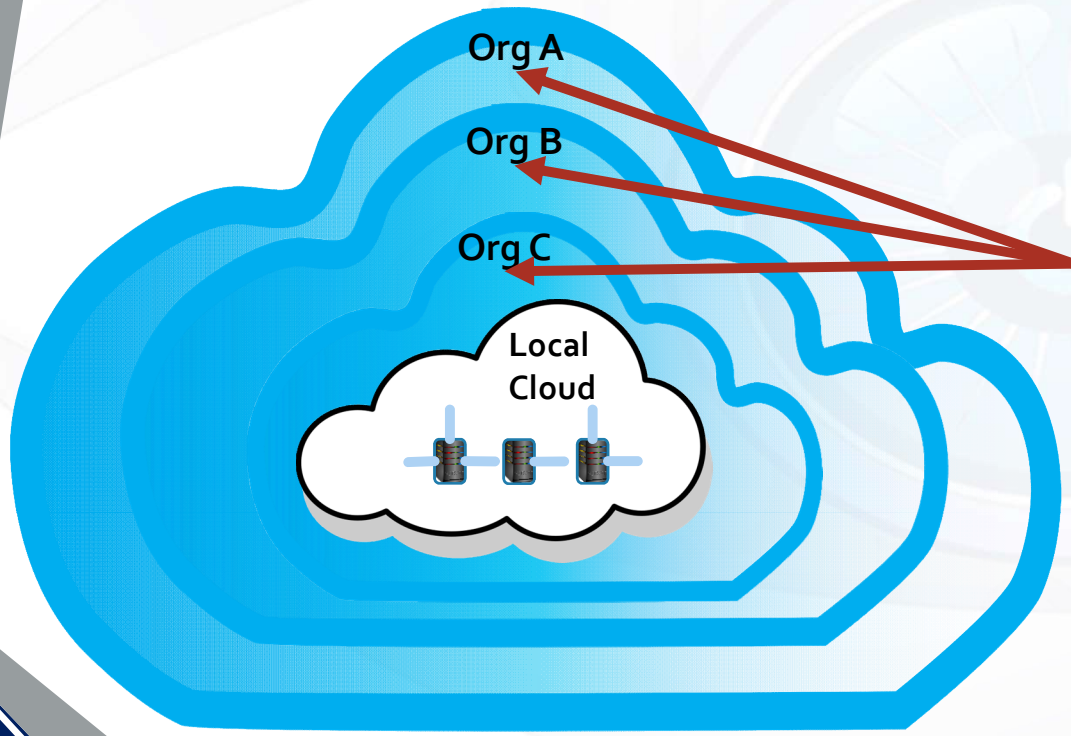
Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organization that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Best OPTION when DATA Security is a Concern and the standards applied to secured the environment can be leveraged among different entities that share a similar objective.

A good example would be the Air's Forces CLOUD One and DISA Cloud Initiatives.

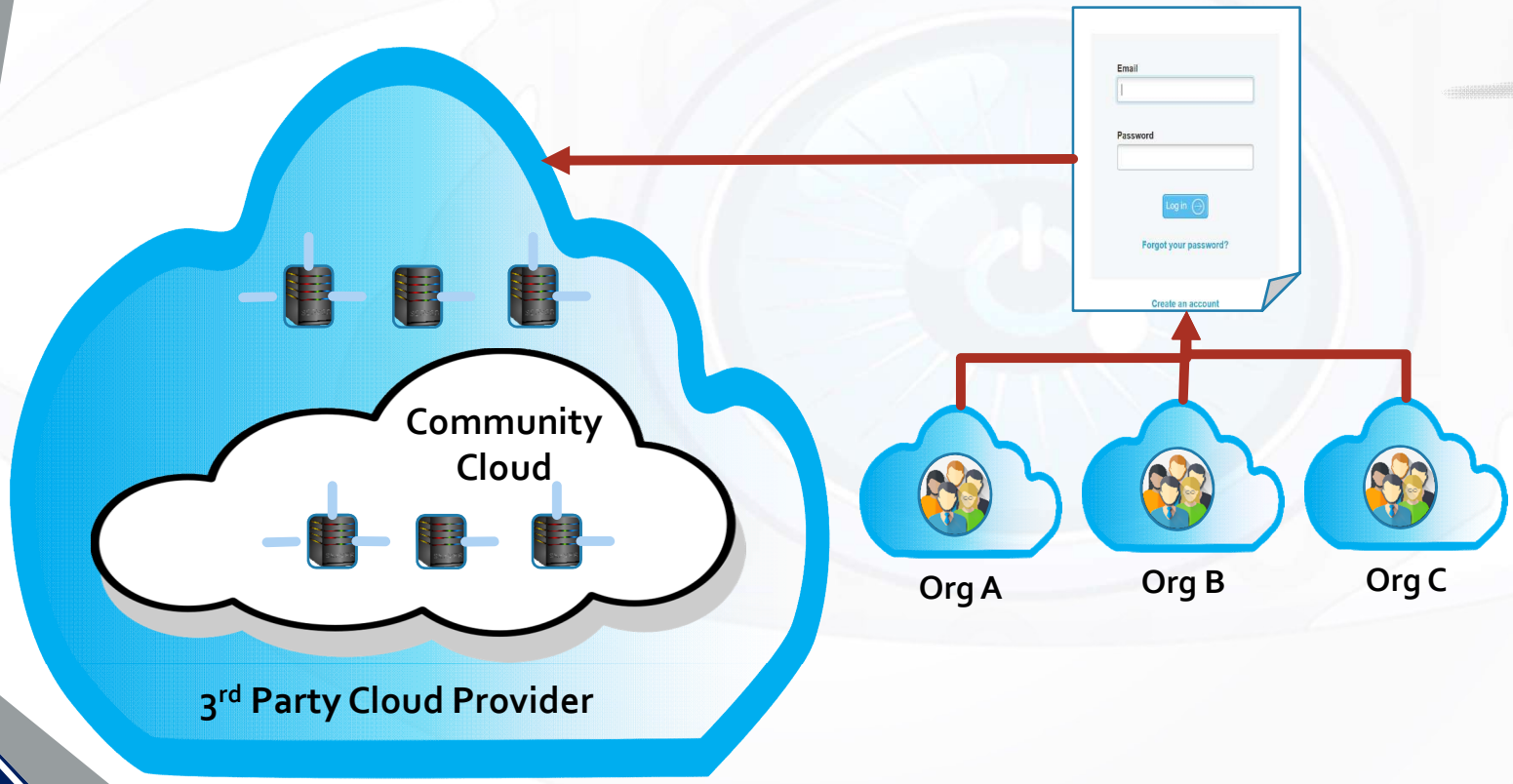
Copyright CyberAdeptness LLC

COMMUNITY ON-SITE CLOUD



Copyright CyberAdeptness LLC

COMMUNITY OFF-SITE CLOUD



Public Cloud

Public Cloud. The cloud infrastructure if provisioned for open use by the general public. It may be owned, managed, and operated by a single business and/or multiple businesses. It exist on the premises of the cloud provider.

Best OPTION when DATA is not a HIGH Concern and/or the information process won't impact the organization's Reputation.

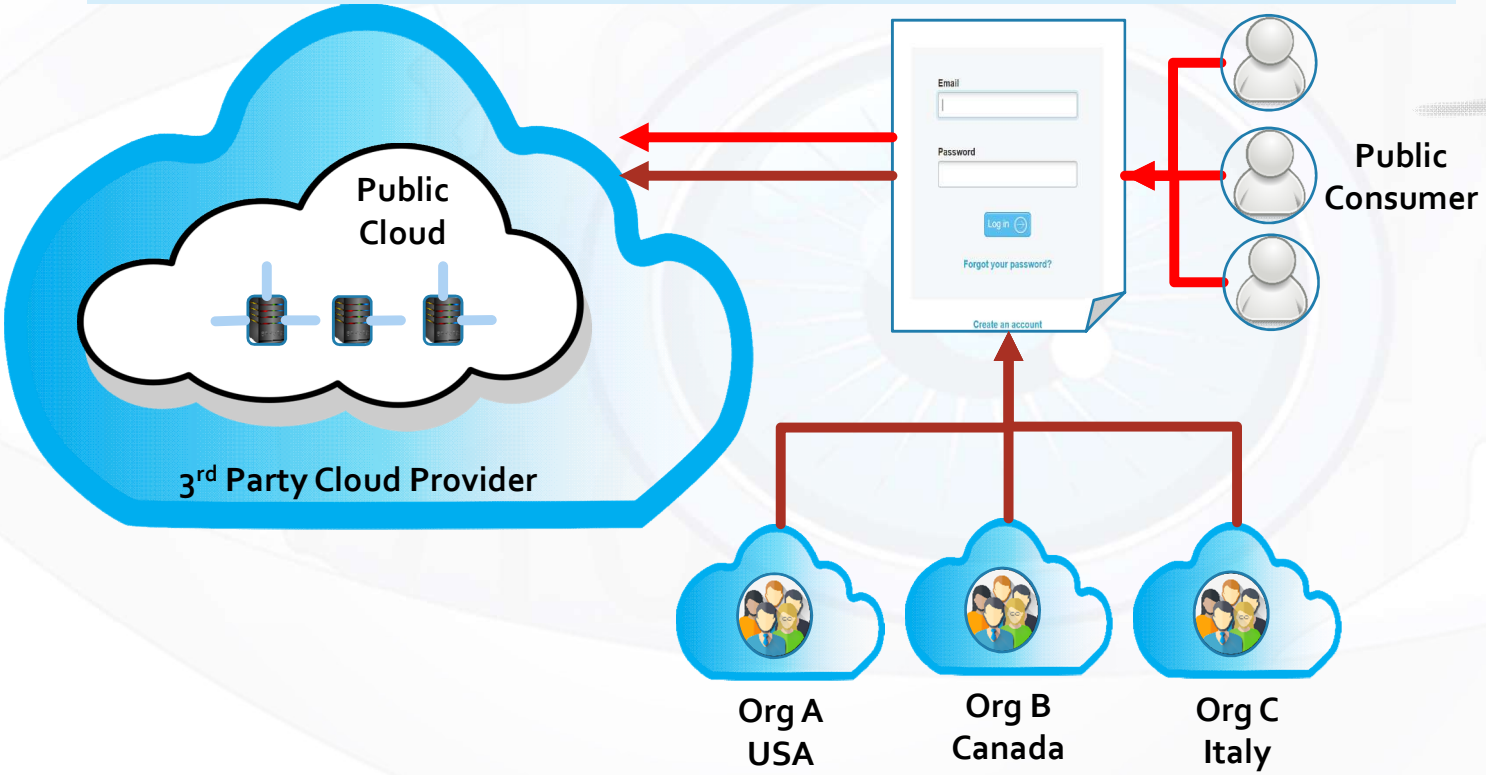
In some instances, Public Clouds may be built in a manner that mimics a community cloud- meaning they comply with a high number of security standards that have an impact on many small size business organizations. In such case, the data to be hosted is typically deemed to have a MODERATE impact within the organization. Security considerations are HIGHLY advice.

A great example of this is MICROSOF OFFICE 365 and GOOGLE Cloud. Both are great alternatives IF the consumer is able to grasp how such needs to be securely configured before deployment.

The KEY here is DATA TYPES stored, processed, or transmitted and the applicable RISK Appetite Level.

Copyright CyberAdeptness LLC

PUBLIC CLOUD



NOTE: In some instances, the Interface displayed differs per consumer. But most of the time the interface is shareable.

Hybrid Cloud

Copyright CyberAdeptness LLC

Hybrid Cloud. The cloud infrastructure is a composition of two or more distinct cloud deployment models (i.e., private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

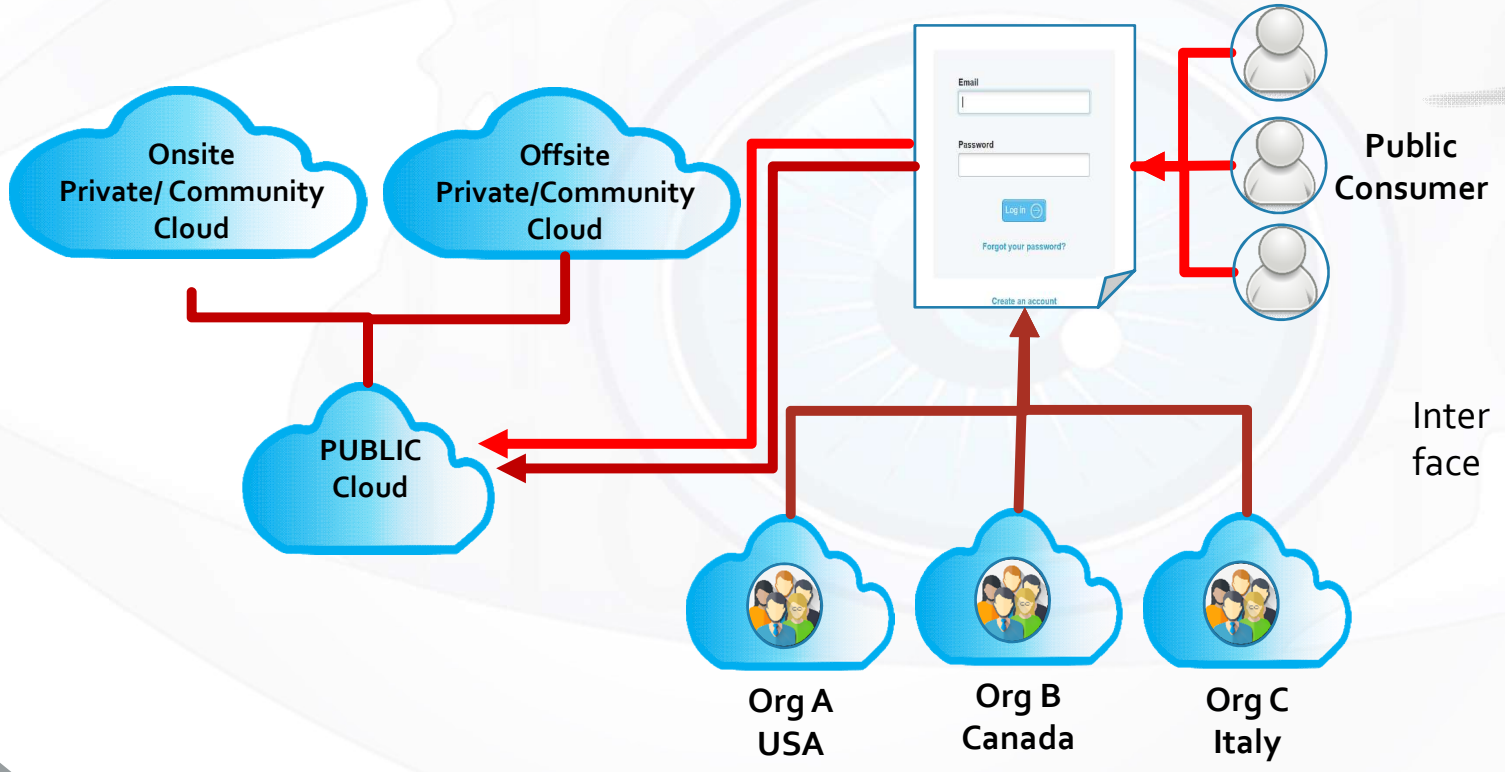
Best OPTION when DATA is not a HIGH Concern and/or the information process requires public input and/or external coordination among teams across the world, in which case, how this is architected and engineered needs to be carefully drafted.

Any lack of security can have a major impact on the organization, as an attacker could infiltrate the organization's internal network. Not recommended for systems deemed to have a HIGH RISK to the organization unless it is built among highly trusted partners.

A good example of this would be– Air Force Cloud One and DISA Cloud Initiatives and many sites that require integration between different sectors to function properly.

Copyright CyberAdeptness LLC

HYBRID CLOUD



NOTE: In some instances, the Interface displayed differs per consumer. But most of the time the interface is shareable.

Cloud Models

At a Glance

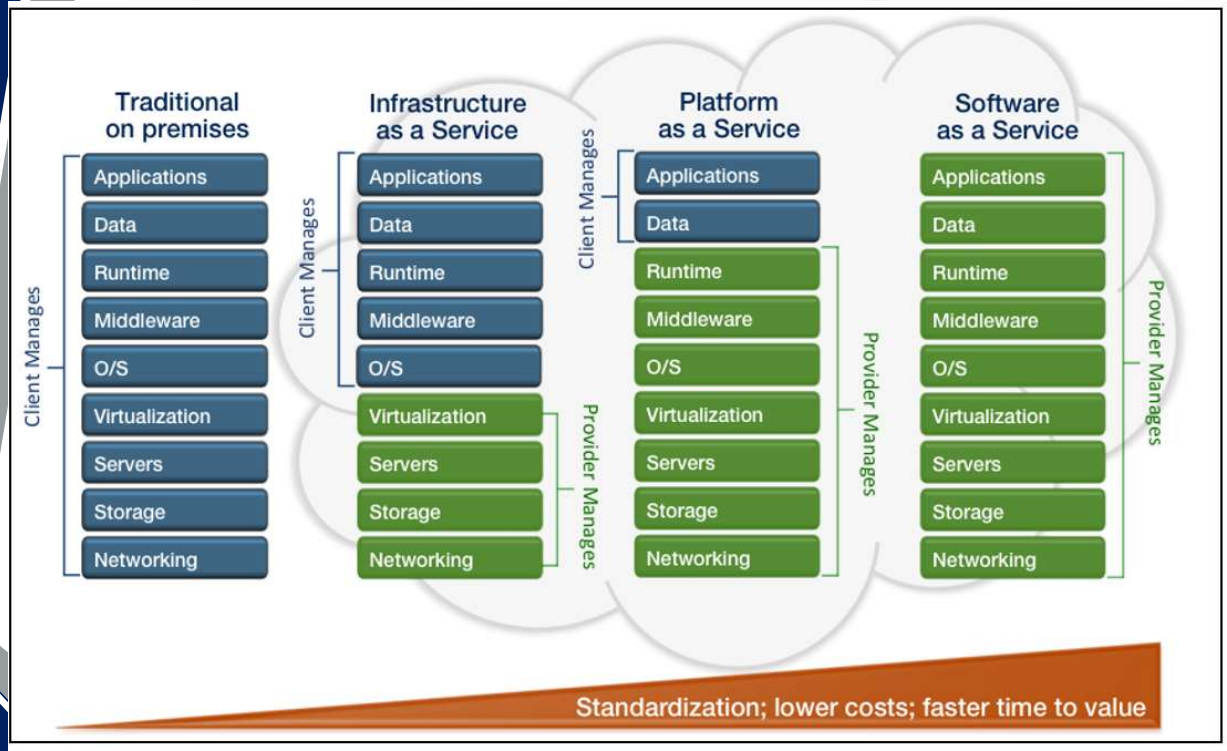
Copyright CyberAdeptness LLC

GENERAL CHARACTERISTICS

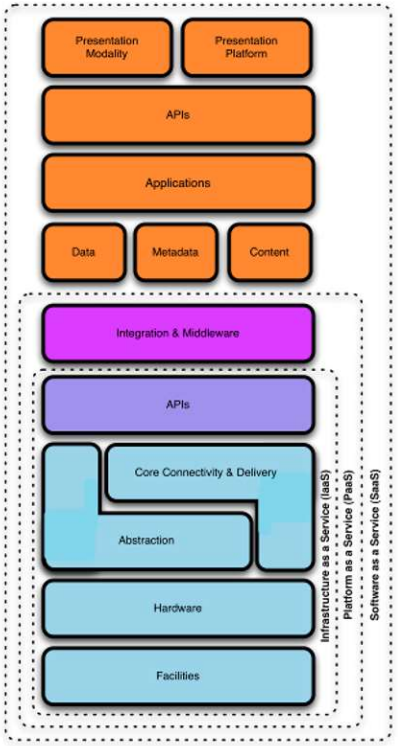
Service Model	General Characteristics
SaaS	▪ They are usually deployed as hosted services and are accessed via a network connecting SaaS consumers and providers. ▪ The SaaS consumers can be organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users. ▪ SaaS consumers access and use applications on demand, and can e billed on the number of consumers or the amount of consumed services. ▪ If billed on the amount of consumed services, it can be measured in terms of the time in use, the network bandwidth consumed, or the amount/duration of data stored.
PaaS	▪ Cloud consumers employ the tools and execution resources provided by cloud providers for the purpose of developing, testing, deploying, and managing applications hosted in a cloud system. ▪ Consumers can be application developers who design and implement application software, application testers who run and test application in various cloud systems, application deployers who publish applications into a cloud system, and application administrations who configure and monitor application performance on a platform. ▪ Consumers can be billed by the number of consumers, the type of resources consumed by the platform, or the duration of platform usage.
IaaS	▪ Consumers are provisioned with the capabilities to access virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources, on which consumers can deploy and run arbitrary software. ▪ Consumers can be system developers, system administrators, and information technology (IT) managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations. ▪ Consumers are provisioned with the capabilities to access these computing resources, and are billed for the amount of resources consumed.

Copyright CyberAdeptness LLC

CLOUD MODELS AT A GLANCE



Reference: CSCC Practical Guide to PaaS v1.0



Reference: CSCC Security Guidance for Critical Areas of Focus in Cloud Computing v3.0

VISUAL CLOUD MODELS OVERVIEW

Managed by Provider (s)

Applications

SaaS

Software
As A Service

Runtime

Middleware

O/S

PaaS

Platform
As A Service

Networking

Servers

Storage

Hypervisor

IaaS

Infrastructure
As A Service

Managed by Consumer

The areas managed by the consumer truly depend on the model selected.

They can managed all items noted under provider, or manage both or one of the top layers displayed (i.e., PaaS or SaaS).

But one thing is for certain--- all consumers are fully responsible for the following:

Data

Copyright CyberAdeptness LLC

WHAT ARE THE CAPABILITIES

Infrastructure As A Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

This is the MOST IMPORTANT LAYER as it is where the physical server resides.

The Security of PaaS and SaaS will depend on the security applied at this layer at a physical and logical level.

Platform As A Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

The hallmark of a PaaS system is the ability for the consumer to create and run applications and services that meet specific business needs.

Software As A Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

NOTE: Container As A Service (CaaS) *is a new model* that was not part of the original models delineated for Cloud.

That said, while it can be integrated to a hypervisor structure, it is not dependent on such– therefore it won't be addressed on this presentation.

Please review the ***Container As A Service (CaaS)*** documentation for additional information.

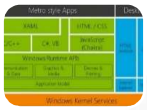
1st Layer → 2nd Layer → 3rd Layer

Copyright CyberAdeptness LLC

HOW ARE MODELS MANAGED

Managed by Provider (s)

Applications



Runtime

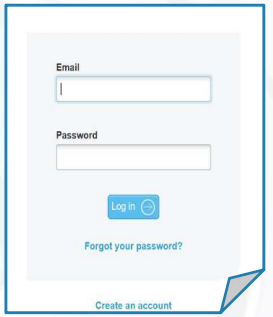
Middleware

O/S

SaaS
Software
As A Service

PaaS
Platform
As A Service

End-User Interface



Networking

Servers

Storage

Hypervisor

IaaS
Infrastructure
As A Service

The key item on all cloud models is the ***Service Interface*** between the provider and the Consumer, which is key to defining the characteristics of the cloud service.

This service interface is essential to ensure both the CSP and authorized Consumer have a common interface in which to address the requirements set-forth on the *Service Level Agreement (SLA)* to include response and performance.

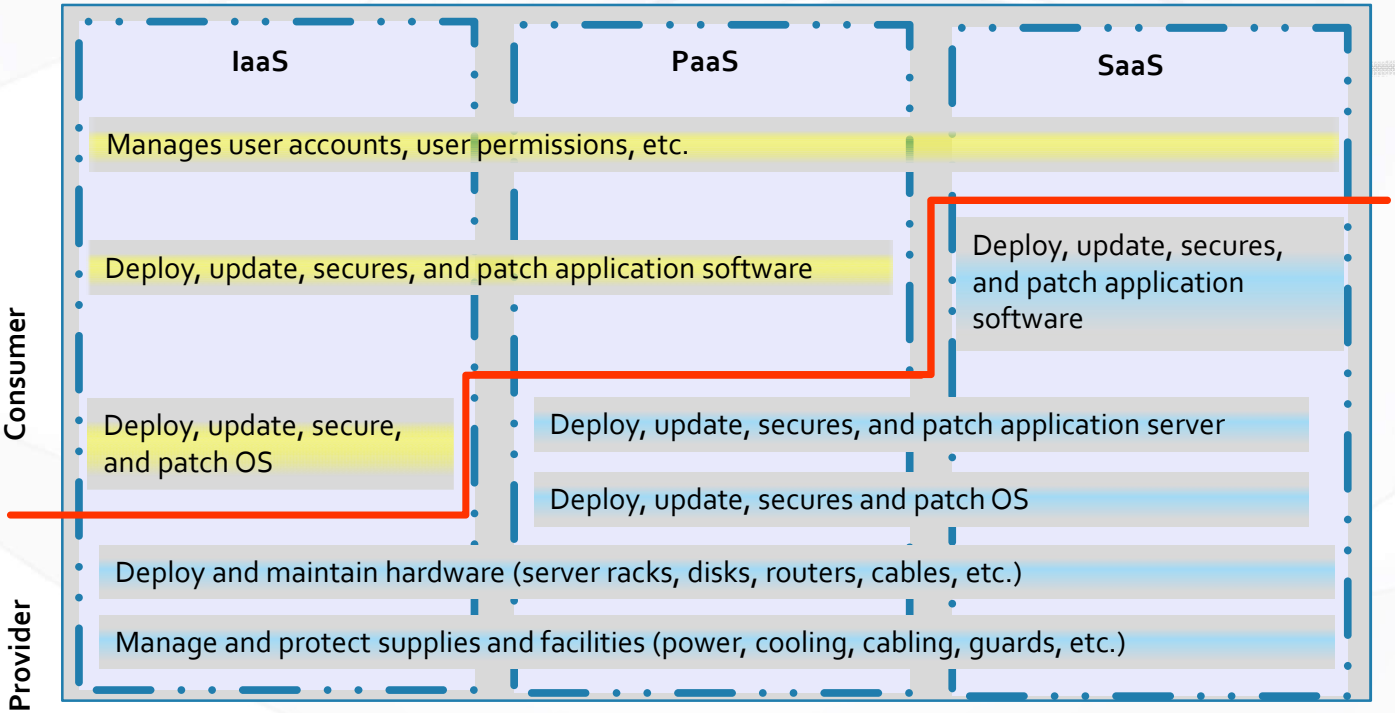
Copyright CyberAdeptness LLC

Security

At a Glance

Copyright CyberAdeptness LLC

HOW IS SECURITY OUTSOURCED



Note: Breakdown attained from Cloud Security Alliance documentation, slightly modified by CyberAdeptness LLC

WHO CONTROLS SECURITY VISUAL

Control over how systems must be secured within the cloud are impacted by the Cloud Model & Deployment methodology used. The SPI (SaaS, PaaS, IaaS) Models varies from CSP to CSP… while some may include it as part of the overall package, others may offer it as a service. The following graphic provides an overview of the general architecture levels and associated control level.

Provider	Consumer	SaaS	Provider	Consumer	PaaS	Provider	Consumer	IaaS	Provider	Consumer	Serverless/ API
M	L	Application	M	L	Application	N	F	Application	F	N	Application
F	N	Middleware	M	L	Middleware	N	F	Middleware	F	N	Middleware
F	N	Guest OS	F	N	Guest OS	N	F	Guest OS	F	N	Guest OS
F	N	Hypervisor	F	N	Hypervisor	F	N	Hypervisor	F	N	Hypervisor
F	N	Storage	F	N	Storage	F	N	Storage	F	N	Storage
F	N	Hardware	F	N	Hardware	F	N	Hardware	F	N	Hardware
F	N	Network	F	N	Network	F	N	Network	F	N	Network

L = Limited control **M** = Most Control
N= No control **F** = Full Control

Note: Breakdown attained from ***Securing the Cloud Book*** by Vic Winkler, slightly modified by CyberAdeptness LLC

Copyright CyberAdeptness LLC

WHO CONTROLS SECURITY

97% of consumers are oblivious how security functions within a cloud, unless they have had hands on a government project and ***70% of providers*** don't fully grasp how cloud services function, they simply see an opportunity for a quick Return On Investment (ROI) Turn around with minimal consideration on the consumer.

Security within a cloud can be controlled by MULTIPLE Actors, and these leads to MAJOR issues within the cloud when NOT Engineered Correctly. The Actor responsible for Infrastructure As A Service (IaaS) is extremely important, as all other services WILL BE IMPACTED. Surely, Security among all layers is KEY for a Defense In-depth strategy, but truly grasping what the consumer is signing up for can alleviate headaches.

This is why before using a cloud environment, organizations, regardless of size, must perform a risk analysis.

Copyright CyberAdeptness LLC

FINAL THOUGHTS

- Before acquiring cloud services… determine the level of risk deemed acceptable.
- Identify the standards impacting your organization and/or your consumers.
- Determine the Cloud Deployment Model that best suits the organization's needs.
- Determine the Cloud Model that best suits the business objective.
- Identify possible Cloud Service Provider (CSPs) alternatives and determine if they comply with the standards impacting your organization and/or consumer sector.
- Identify number of actors involved in the cloud ecosystem and the impact it may have in your organization.
- Identify the cloud deployment models supported by the CSP.

Copyright CyberAdeptness LLC

Send them to
info@cyberadeptness.com

Need Help?

We have over 20+ years of combined experience in the field and a unique process to streamline the requirements.

Contact us today to schedule a meeting and determine how we may be of help to your organization. Our processes are flexible to accommodate compliance needs, regardless of sector (i.e., Healthcare, Finance, Law, Education, etc.).

References

- **Everything VM: History of Virtualization-** http://www.everythingvm.com/content/history-virtualization
- **Cloud Security Alliance- Security Guidance for Critical Areas of Focus in Cloud Computing v3.0-** https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- **NIST SP 500-292 : NIST Cloud Computing Reference Architecture-** http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf
- **ENISA 2013 Security Framework for Governmental Clouds-** https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds
- **ENISA 2015 Cloud Security Guide for SMEs** - https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes
- NIST SP 500-299: NIST Cloud Computing Security Reference Architecture

Copyright CyberAdeptness LLC