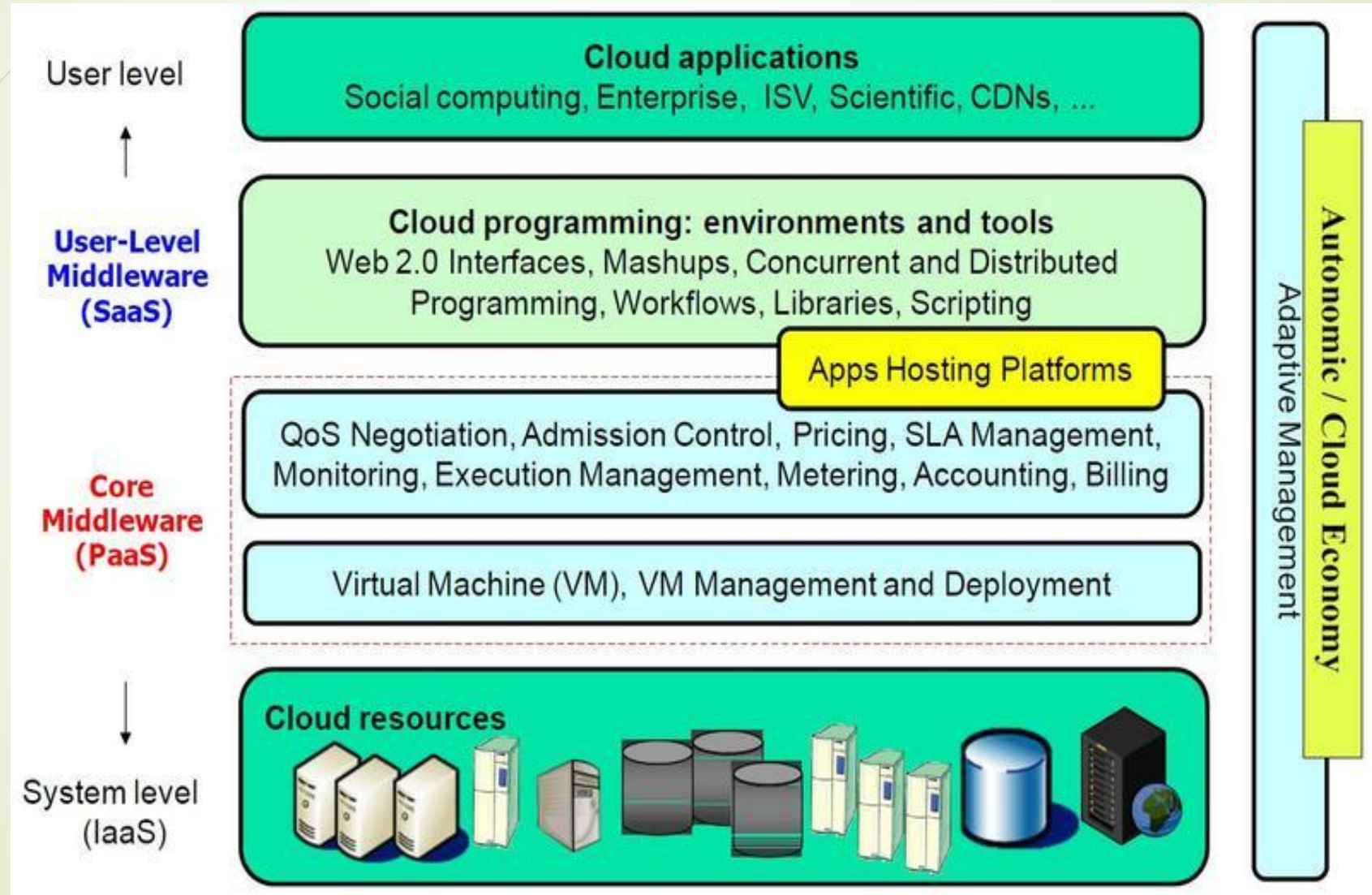





Unit 2 – Cloud Computing Architecture

Cloud Computing Architecture





Category	Characteristics	Product Type	Vendors
SaaS	Customers are provided with applications that are accessible anytime and from anywhere	Web applications and services (Web 2.0)	SalesForce.com Clarizen.com Google Apps
PaaS	Customers are provided with a platform for developing applications hosted in the Cloud	Programming APIs and frameworks; Deployment Systems	Google AppEngine Microsoft Azure Data Synapse
IaaS	Customers are provided with virtualized hardware and storage on top of which they can build their infrastructure	Virtual machines management infrastructure; Storage & Network management	Amazon EC2; GoGrid; Nirvanix

Cloud-Computing Services Classification



Infrastructure as a Service (IaaS)

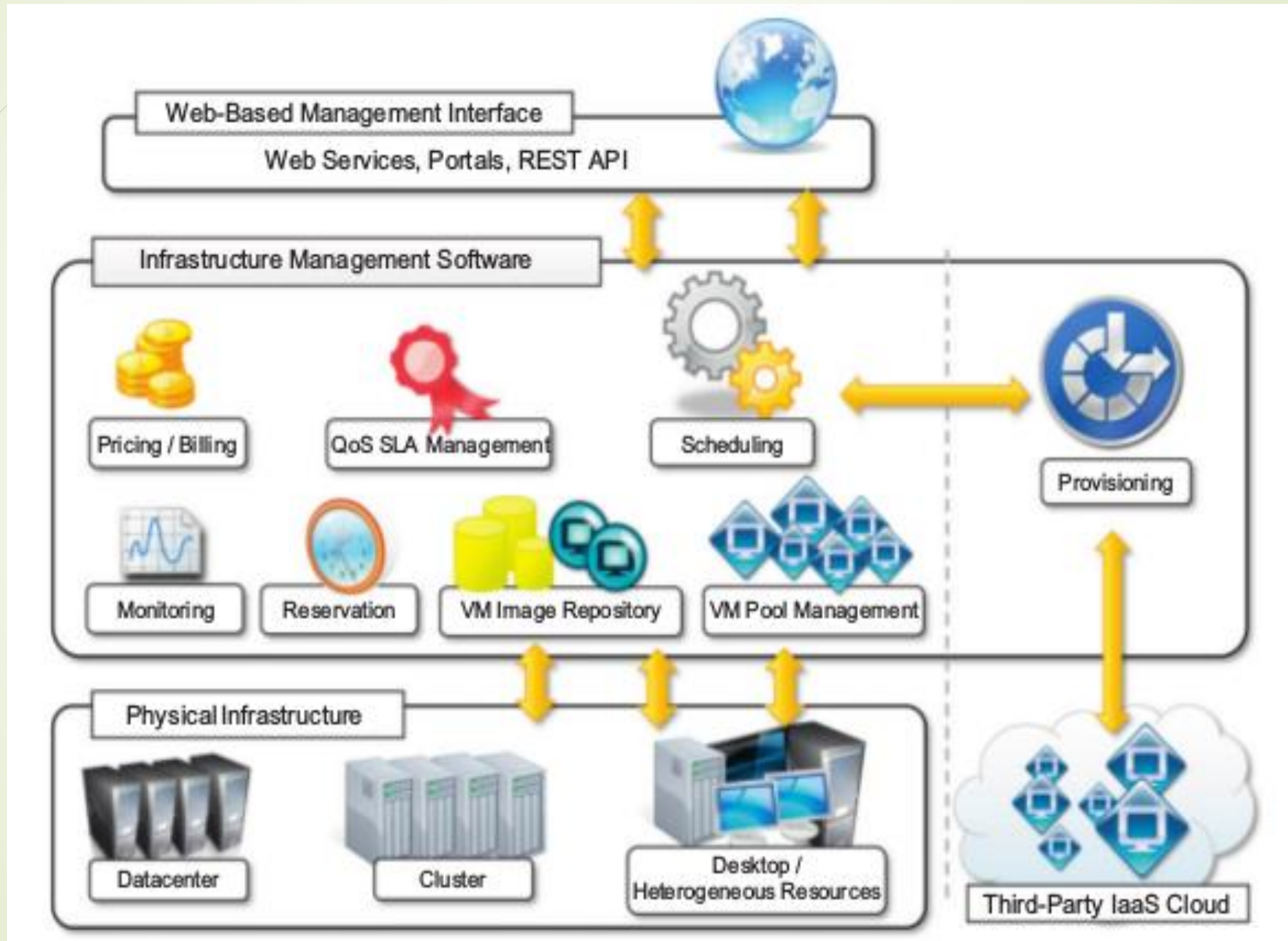
- Most popular & developed market segment
- Delivers customizable infrastructure on demand
- Single servers, network devices, load balancers, database & web servers
- **Hardware virtualization** – One or more virtual machines configured to define the distributed system on top of which applications are installed & deployed



IaaS (contd.)

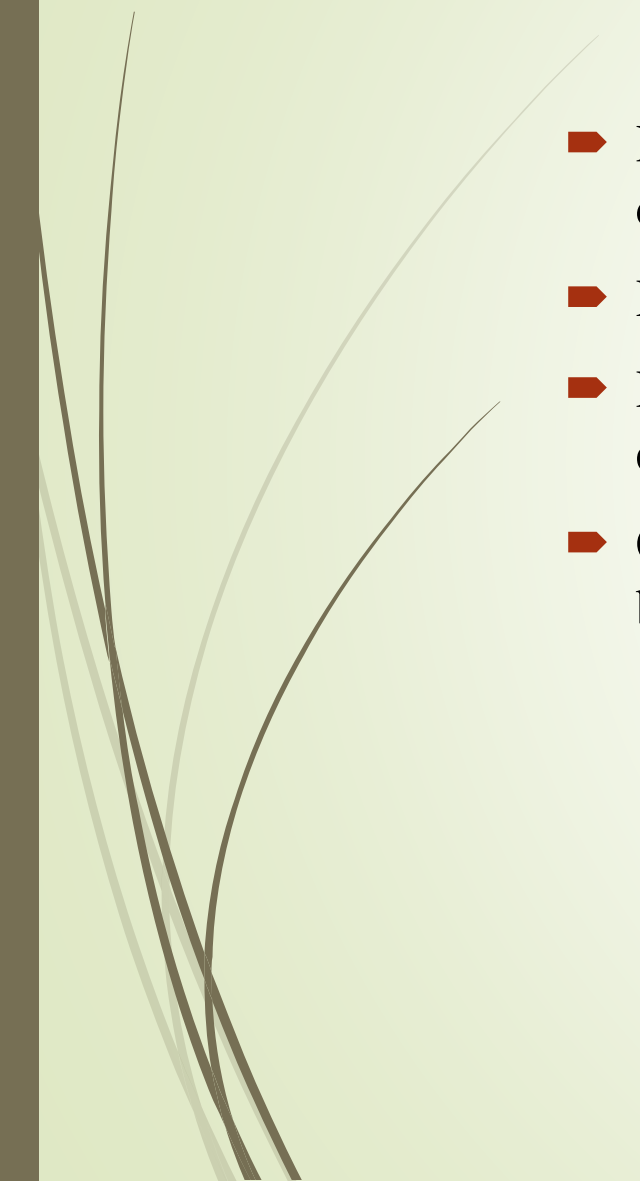
- Infrastructure can be **heterogeneous** in nature
- **Middleware** – To provide an appropriate runtime environment for applications and to utilize resources at best
- **Virtualization** – To guarantee runtime environment customization, application isolation, sandboxing & quality of service
- **Hypervisors** manages the pool of resources and expose the distributed infrastructure as a collection of virtual machines
- **Virtualization** is paired with storage and network strategies to allow the infrastructures to be completely virtualized and controlled

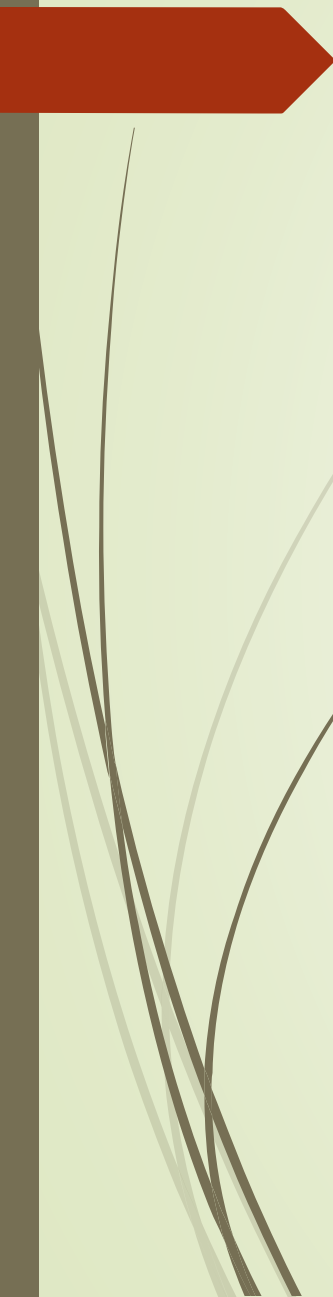
IaaS (contd.)





Platform as a Service (PaaS)

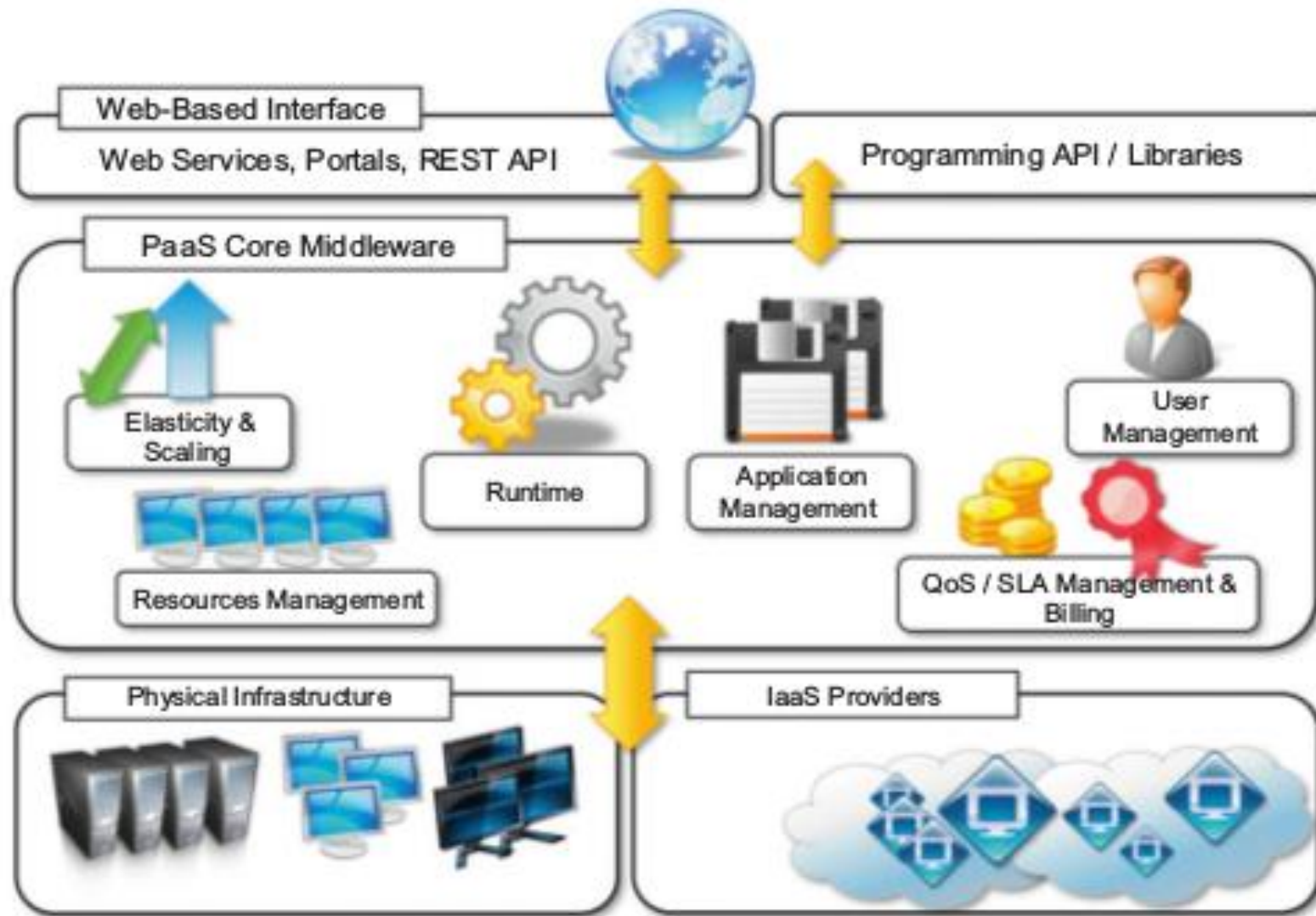
- Provides a development & deployment platform for running applications in the cloud
 - PaaS constitutes the middleware on top of which applications are built
 - PaaS implementations provide applications with a runtime environment and don't expose any service for managing infrastructures
 - Configuring application components & supporting technologies, managing system based on the policies set by the user
- 



Category	Description	Product Type	Vendors
PaaS – I	Runtime environment with web hosted application development platform	Middleware+Infrastructure Middleware+Infrastructure	Force.com Longjump
PaaS – II	Runtime environment for scaling web applications	Middleware+Infrastructure Middleware Middleware+Infrastructure Middleware+Infrastructure Middleware	Google AE AppAcale Heroku Engine Yard GigaSpaces
PaaS – III	Middleware & programming model for developing applications in the cloud	Middleware+Infrastructure Middleware	MS Azure Cloud IQ

Platform as a Service Offering Classification

PaaS (contd.)

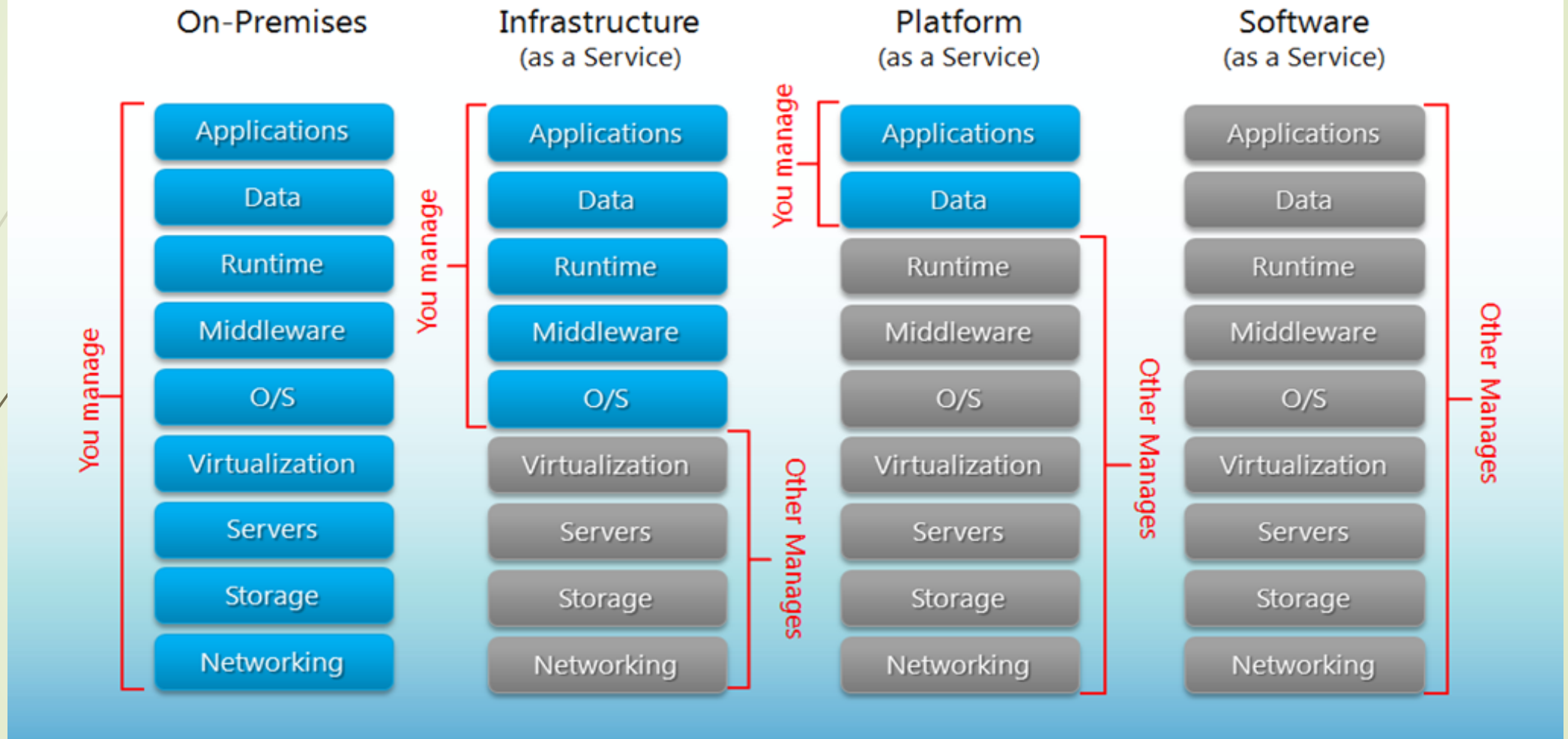




Software as a Service (SaaS)

- SaaS is a way of delivering applications over the Internet; as a service
- Web-based software, on-demand software, or hosted software
- Characteristics
 - Multi-tenancy in nature – One to many
 - Centrally managed
 - Easy customization
 - Better Access

Separation of Responsibilities



IaaS, PaaS, SaaS; Separation of Responsibilities

Cloud Computing Service Layers

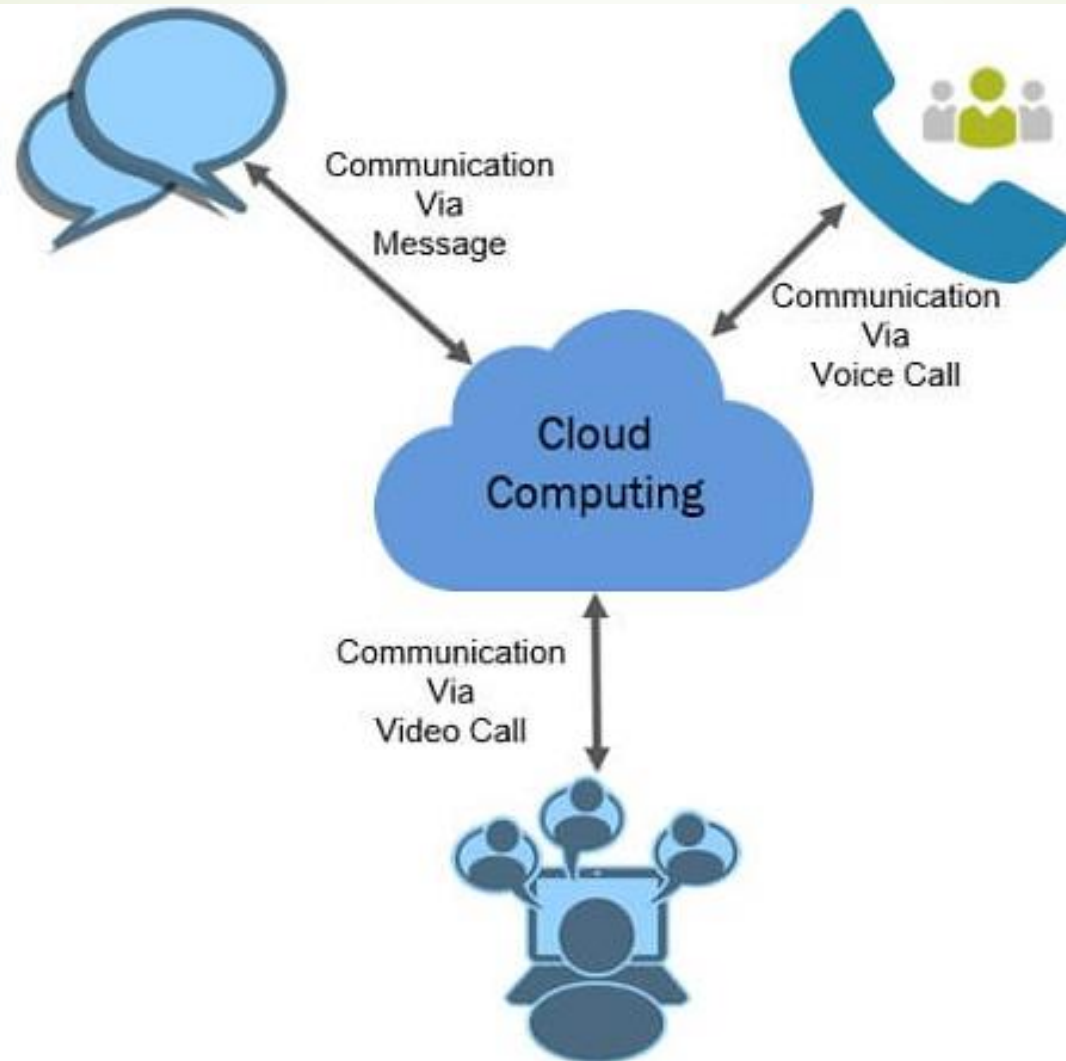
Services		Description
Application Focused	Services	Services – Complete business services such as PayPal, OpenID, OAuth, Google Maps, Alexa
	Application	Application – Cloud based software that eliminates the need for local installation such as Google Apps, Microsoft Online
	Development	Development – Software development platforms used to build custom cloud based applications (PAAS & SAAS) such as SalesForce
Infrastructure Focused	Platform	Platform – Cloud based platforms, typically provided using virtualization, such as Amazon ECC, Sun Grid
	Storage	Storage – Data storage or cloud based NAS such as CTERA, iDisk, CloudNAS
	Hosting	Hosting – Physical data centers such as those run by IBM, HP, NaviSite, etc.



Communication as a Service (CaaS)


- An outsourced enterprise communications solution that can be leased from a single vendor
- Such communications can include voice over IP (VoIP or Internet telephony), instant messaging (IM), collaboration and videoconference applications using fixed and mobile devices
- CaaS has evolved along the same lines as Software as a Service (SaaS)
- CaaS brings social networking, cloud computing, and smartphones together, providing cloud technologies that let users communicate via voice, text, and rich media on whatever device they prefer to use.

CaaS (contd.)



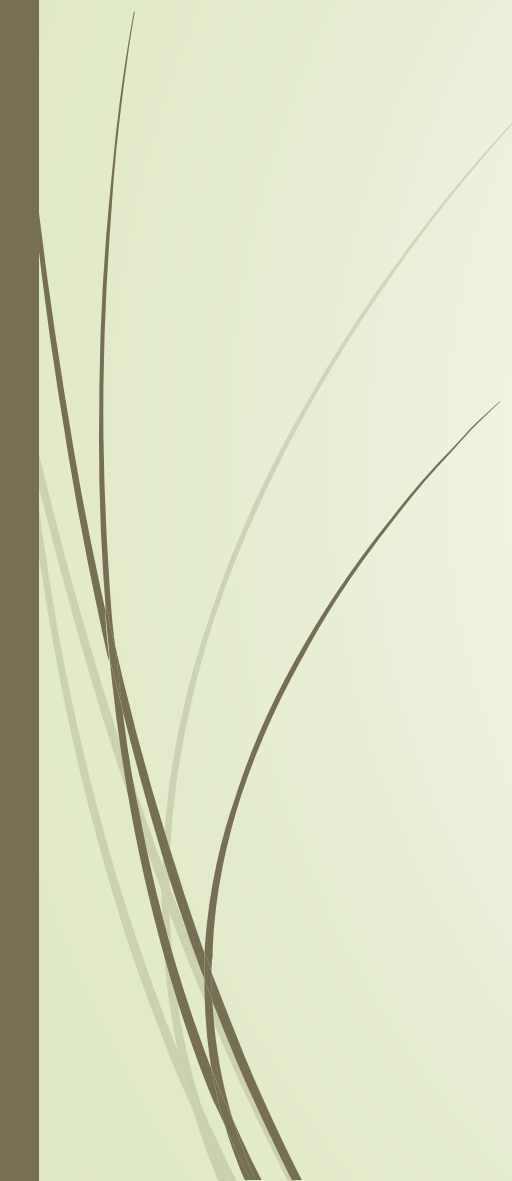


Unified Communication

- Communications integrated to optimize business performance
 - Can describe a seamless set of voice, video and Web collaboration applications designed to enable advanced connectivity between employees, customers, partners and other stakeholders available on any device
 - In the large enterprise setting, Unified Communications allow employees to send and receive messages on various medium – guided or switching
- 



Modern On-Demand Computing

- Computing resources are made available to the user as needed
 - The resources may be maintained within the user's enterprise, or made available by a service provider
 - The on-demand model evolved to overcome the challenge of being able to meet fluctuating resource demands efficiently
 - Computer Associates, HP, IBM, Microsoft, and Sun Microsystems are among the more prominent on-demand vendors
 - The major advantage of On Demand Computing (ODC) is low initial cost, as computational resources are essentially rented when they are required. This provides cost savings over purchasing them outright
- 

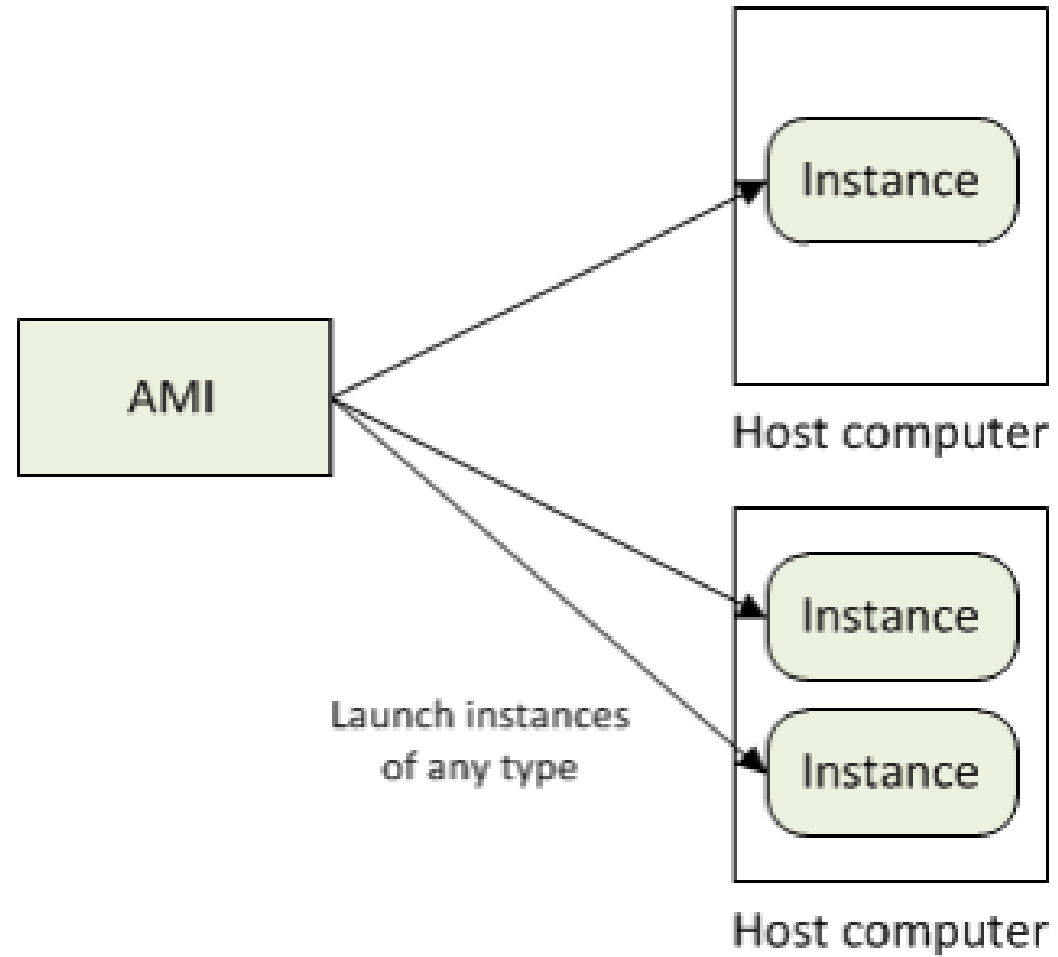


Amazon Web Services

Amazon Elastic Compute Cloud (Amazon EC2)

- EC2 is a Web service with a smooth interface for launching part of an application under several operating systems
- EC2 allows users to rent virtual computers on which to run their own computer applications
- EC2 allows a user to load instances of an application with a custom application environment, manage networks access permissions, and run the images using as many or as few systems as desired
- EC2 instances boot from an AMI (Amazon Machine Image) digitally signed and stored in Amazon Simple Storage Service (Amazon S3)
- A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, hence the term "elastic"

EC2 (contd.)





Characteristics of EC2

- Persistent Storage
 - Elastic IP Addresses
 - Amazon Cloud Watch
 - Automated Scaling
 - Reliability
- 



Elastic IP Addressing

- To use an Elastic IP address, you first allocate one to your account, and then associate it with your instance or a network interface.
- When you associate an Elastic IP address with an instance or its primary network interface, the instance's public IPv4 address (if it had one) is released back into Amazon's pool of public IPv4 addresses. You cannot reuse a public IPv4 address.
- You can disassociate an Elastic IP address from a resource, and reassociate it with a different resource
- A disassociated Elastic IP address remains allocated to your account until you explicitly release it
- To ensure efficient use of Elastic IP addresses, we impose a small hourly charge if an Elastic IP address is not associated with a running instance, or if it is associated with a stopped instance or an unattached network interface



Elastic IP Addressing (contd.)

- While your instance is running, you are not charged for one Elastic IP address associated with the instance, but you are charged for any additional Elastic IP addresses associated with the instance.
- An Elastic IP address is for use in a specific region only
- When you associate an Elastic IP address with an instance that previously had a public IPv4 address, the public DNS hostname of the instance changes to match the Elastic IP address
- We resolve a public DNS hostname to the public IPv4 address or the Elastic IP address of the instance outside the network of the instance, and to the private IPv4 address of the instance from within the network of the instance
- If your account supports EC2-Classic, the use and behavior of Elastic IP addresses for EC2-Classic and EC2-VPC may differ



Monitoring as a Service (MaaS)

- Monitoring as a service is an outsourced provisioning of security, that leverages the Internet to conduct business.
- MaaS provides protection against Internal as well as external threats
- MaaS Provides services such as early detection, platform service and control monitoring, continuous system
- Offers 24/7 monitoring in real-time and nearly urgent incident response across the security infrastructure that they help to protect vital information assets of their customers in patching and upgrading for fortification




Protection against Internal and External Threats

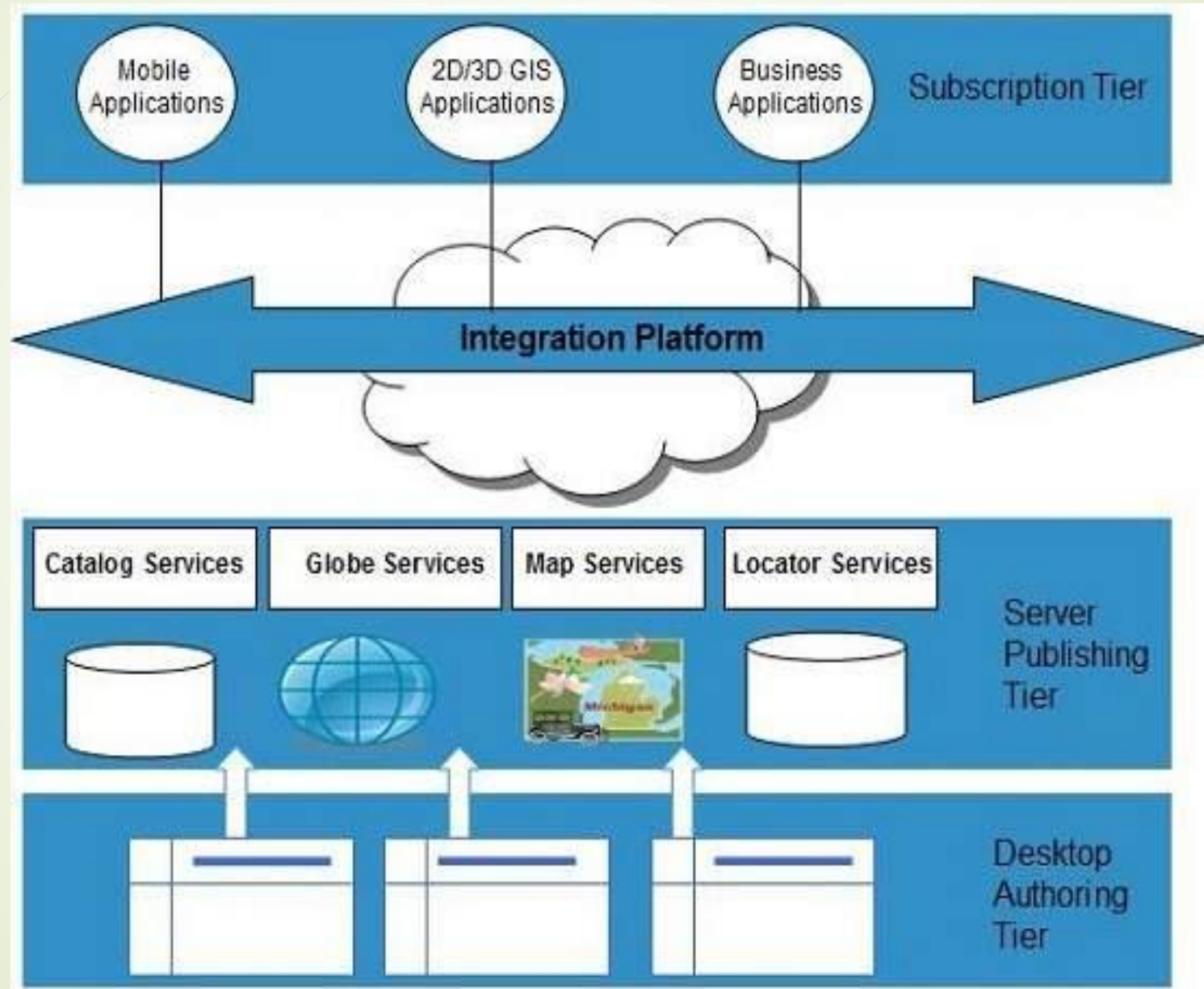
- Early Detection
- Platform, Control, and Services Monitoring
- Intelligent Log Centralization and Analysis
- Vulnerabilities Detection and Management
- Continuous System Patching/Upgrade
- Intervention, Forensics, and Help Desk Services



Service Oriented Architecture (SOA)

- A service is a function that is well-defined, self-contained, and does not depend on the context or state of other services
 - A service-oriented architecture is essentially a collection of services
 - These services communicates with each other
 - SOA defines how to integrate widely disparate applications for a Web-based environment and uses multiple implementation platforms
 - Rather than defining an API, SOA defines the interface in terms of protocols and functionality
- 

SOA (contd.)





SOA vs CC

- SOA convey web services from applications to other programs, and the cloud is about conveying software services to end users and running code



Jericho Cloud Cube Model

- Cloud computing offers a huge possibility for scalability, at almost instantaneous availability and low cost.
- Business managers requires IT operations to assess the risks and benefit this representation of computing model .
- The Jericho forum is an independent group of international information security leaders, have added their input as to how to collude securely in the clouds.
- The Jericho Cloud Cube Model portrays the multidimensional elements of cloud computing, that frames not only cloud use cases but also how they are set up and used.



Jericho Cloud Cube Model

- The Jericho Forum's objectives associated to cloud computing are unique – “enabling secure combination in the appropriate cloud formations suited best to the business needs”.
- Protecting our Data
 - *First, it is necessary to categorize our data so as to know what rules must be applied to protecting it*
 - *We only can meet this requirement if we have comprehensively adopted standards for data classification, metadata for cloud.*
 - *With consideration of what security we must apply to our data, we're in a position to take decision on data migration, cloud composition and cloud levels (infrastructure, platform, Software, process, values)*

Jericho Cloud Cube Model

- The Jericho forum has identified 4 gauge for judgement to differentiate cloud formations from each other and manner of their provisions.
- Cloud Cube Model Dimensions
 - *Dimension: Internal (I) / External (E)* *Location*
 - *Dimension: Proprietary (P) / Open (O)* *Ownership*
 - *Dimension: Perimeterised (Per) / De-perimeterised (D-p)*
Architectures *Perimeter*
 - *Dimension: Insourced / Outsourced* *Sourcing*



Dimension: Internal (I) / External (E)

- This dimension defines the physical location of the data such as where does the cloud form we want to use lie, inside or outside your organization's boundaries.
 - *It is Internal If it is within your own physical boundary.*
 - *It is External If it is not within your own physical boundary.*
- For example, while Amazon SC33 would be external at some location “off-site, virtualized hard disks in an organization's data center will be internal.




Dimension: Proprietary (P) / Open (O)

- This is the dimension that represents the state of ownership of the cloud technology, interfaces, services, etc.
 - Proprietary means that the organization that provides the service is keeping the means of arrangement under their ownership.
 - Open clouds use technology that is not proprietary, meaning that there are likely to be more suppliers, and user are not as strained in being able to share your data and using the same open technology collide with selected parties.

Dimension: Perimeterised (Per) / De- perimeterised (D-p) Architectures

- The third dimension represents the “architectural mindset” - are you operating inside your traditional IT perimeter or outside it?
 - *Perimeterised implies continuing to operate within the traditional IT perimeter*
 - *when operating in the perimeterised areas, you may simply extend your own organisation’s perimeter into the external cloud computing domain using a VPN and operating the virtual server in your own IP domain, making use of your own directory services to control access.*
 - *Then, when the computing task is completed you can withdraw your perimeter back to its original traditional position.*

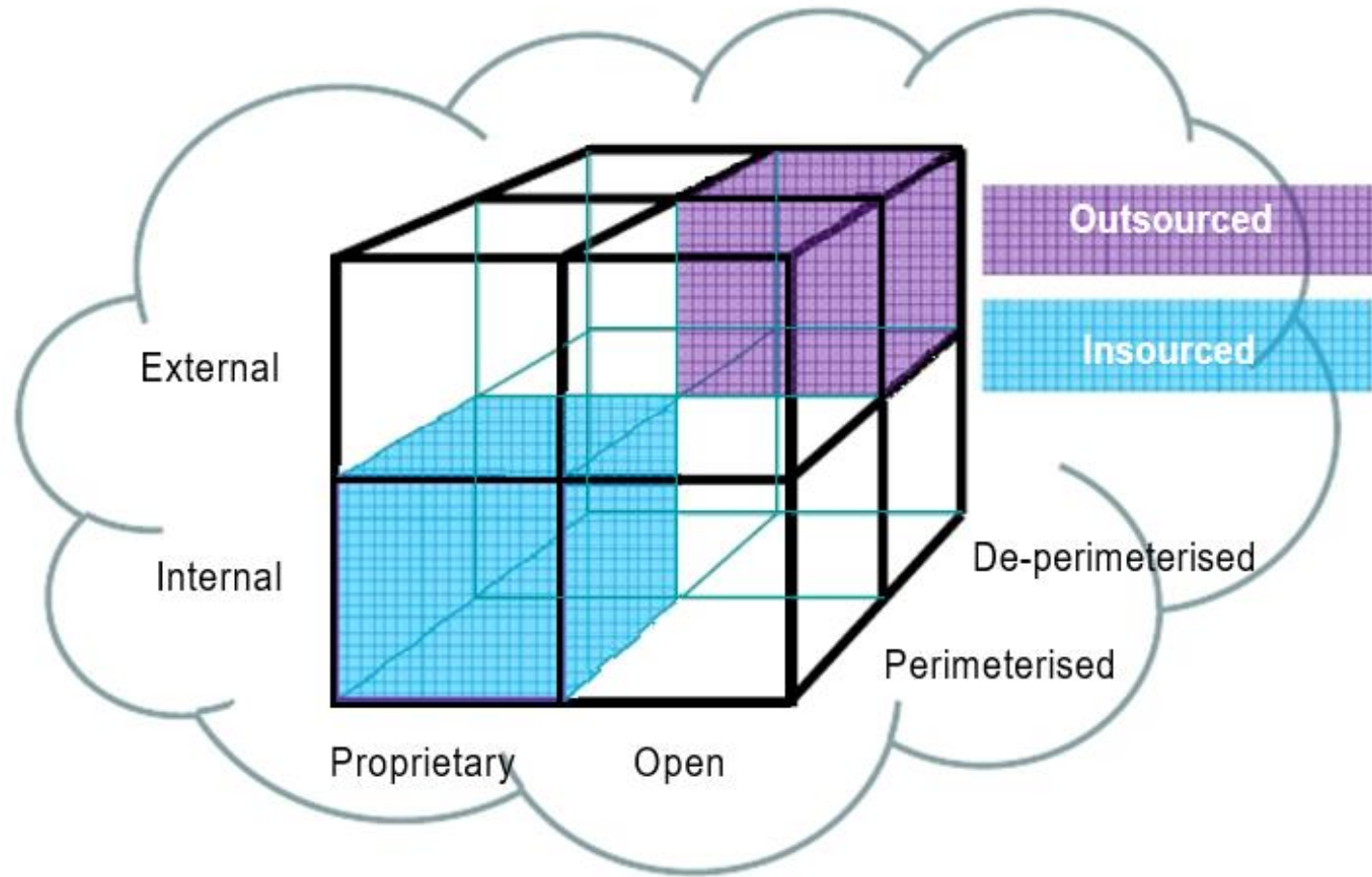


Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures

- De-perimeterised, assumes that the system perimeter is architected following the principles outlined in the Jericho Forum's Commandments and Collaboration Oriented Architectures Framework.
- In a de-perimeterised frame the data would be wrapped with meta-data and mechanisms that from inappropriate usage would protect the data .
- In a de-perimeterised environment an organisation can associate securely with selected parties globally over COA capable network.

Dimension: Insourced / Outsourced

- We define a 4th dimension that has 2 states in each of the 8 cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO), that responds to the question “Who do you want running your Clouds?”:
 - *Outsourced: the service is provided by a 3rd party*
 - *Insourced: the service is provided by your own staff under your control*
- These 2 states describe who is managing delivery of the cloud service(s) that you use.



The Cloud Cube Model



Open-Source Software

