Introduction to Cloud Computing

Srinath Beldona

srinath_beldona@yahoo.com

Agenda

- Pre-requisites
- Course objectives
- What you will learn in this tutorial?
- Brief history – Is cloud computing new?
- Why cloud computing?
- Cloud Computing Definition and Principles

Pre-requisites (1)

- Understanding of basic computer architecture
  - CPU
  - Memory
  - Storage (Volatile and Non-volatile)
- Understanding of basic networking principles
  - Ethernet Switching
  - Basic Routing principles
  - Basic Network security

Pre-requisites (2)

- Understanding of basic security principles
  - Application security
  - Operating system security
  - Device security
- Understanding basics of Virtualization
  - Virtual Machines
  - Hypervisors

What you will learn in this tutorial?

- Basic Cloud computing principles
- Deployment Models
- Service Models
- Economic Considerations
- Operational Characteristics
- Service Agreements including Service Level Agreements
- Cloud Security
- Cloud Risks & compliance
- Recommendations
- How to select a Cloud Provider?
- Conclusion

Brief history: Is cloud Computing New?

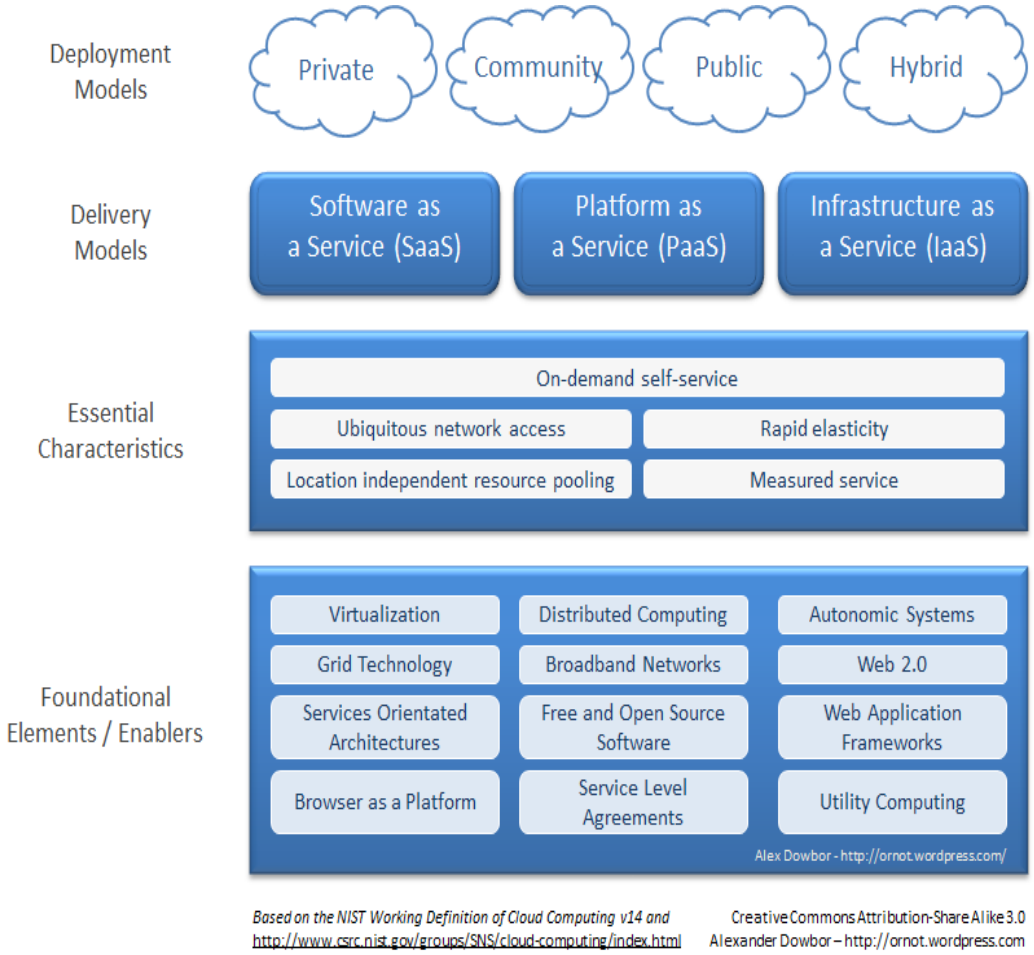
- Utility Computing: 1961
- Time Sharing: 1970s
- Large Distributed Data Centers 1980s-1990s
- Internet Computing 2000-Present
- What is new in cloud computing today?
  - Faster data communication
  - Faster and more reliable computing
  - Denser and cheaper storage
  - Newer Programming paradigms
- Comprehensive Computational resource sharing

Why Cloud Computing is needed?

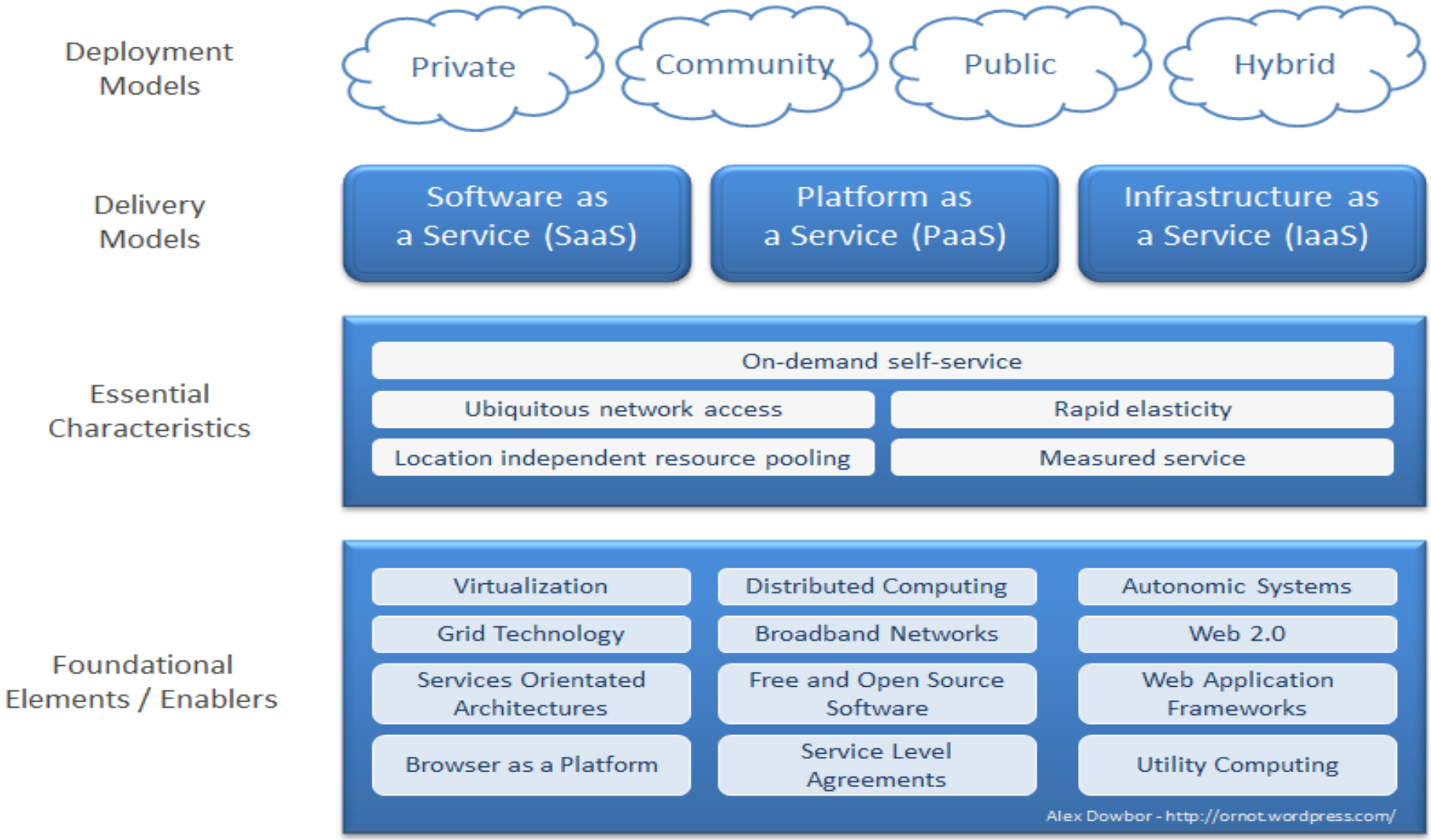
- Value to Consumers
- Value to Vendors
- New Revenue and Jobs

NIST Cloud Computing Model

- Model Organization
  - Five essential characteristics
  - Three Service Models
  - Four Deployment Models



NIST Cloud Computing Model



Based on the NIST Working Definition of Cloud Computing v14 and http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Creative Commons Attribution-Share Alike 3.0
Alexander Dowbor – http://ornot.wordpress.com

Value of NIST Cloud Computing Model

- Why do we need a cloud computing model ?
- Value of the model
  - Cloud Networks configurations and its use
- Major benefits to provider and users
  - Precision
  - Clarity

CLOUD COMPUTING PRINCIPLES

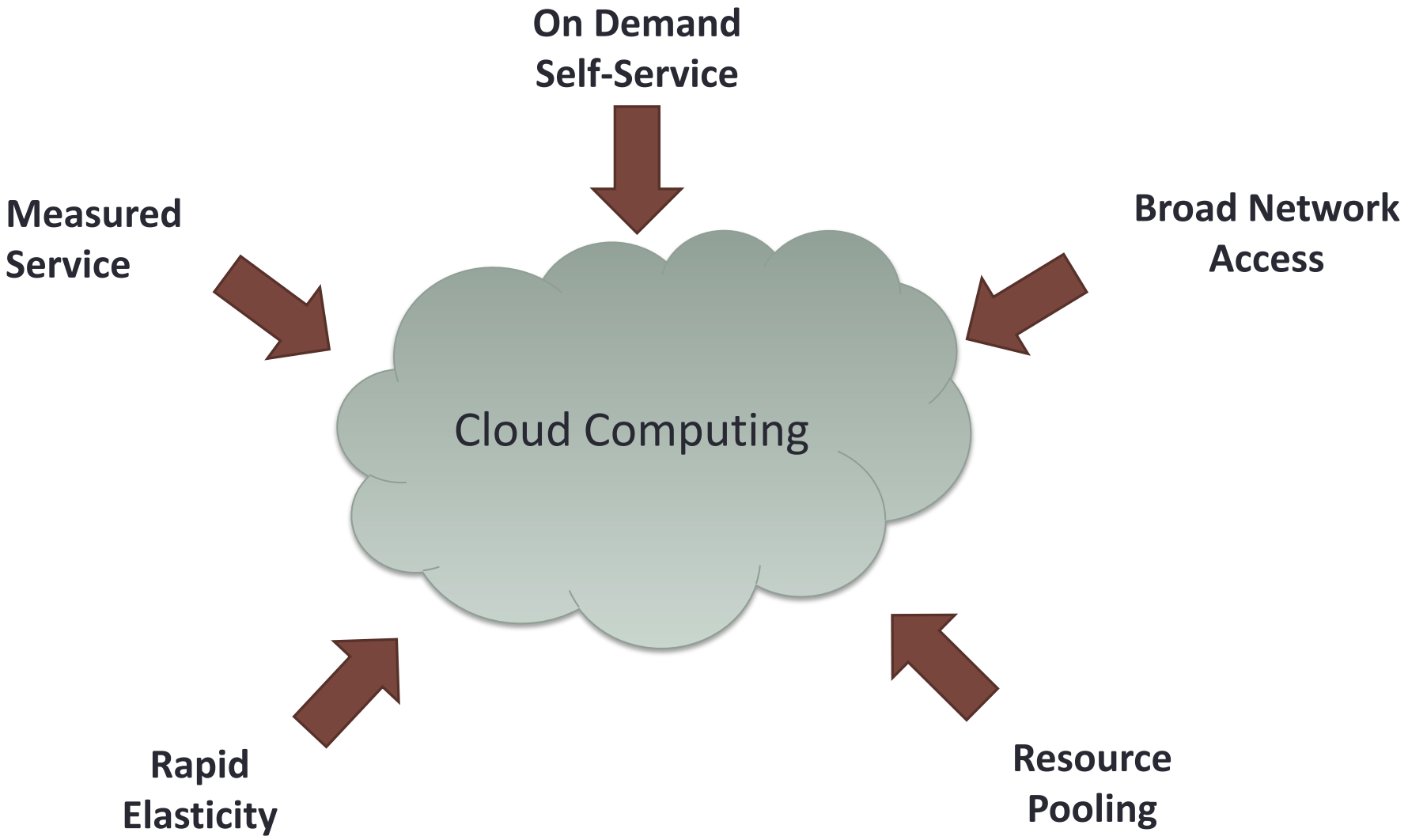
What is Cloud Computing?

- Cloud Computing is a on demand model
- Shared pool of computing resources
  - Servers
  - Storage
  - Applications
  - Services

What is Cloud Computing? (contd.)

- Rapidly provisioned
- Rapidly released
- Minimal Management Effort of Service Providers
- Other definitions also exist

Five Essential Characteristics of Cloud Computing



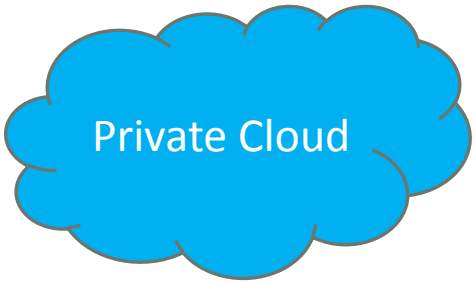
Cloud Service Models

Software as a Service
SaaS

Platform as a Service
PaaS

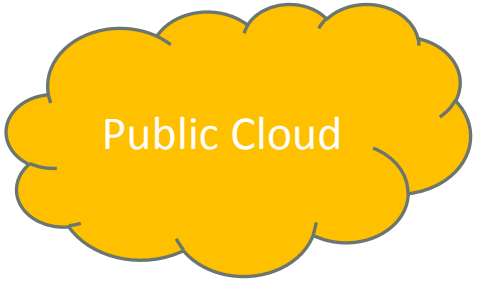
Infrastructure as a Service
IaaS

Deployment Models



Private cloud the cloud infrastructure is

1) **provisioned for exclusive use by a single organization with**
2) **multiple consumers,**
3) **for example individual business units**
4) **owned, managed, and operated by the organization**



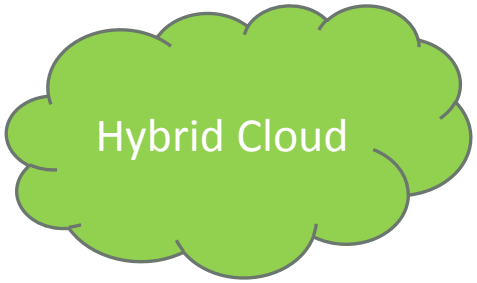
public cloud infrastructure is

1) **provisioned for open use by public**
2) **Owned, managed and operated by a business, government or university**
3) **Mostly in the premises of a cloud provider**

Deployment Models

community cloud for use by a community

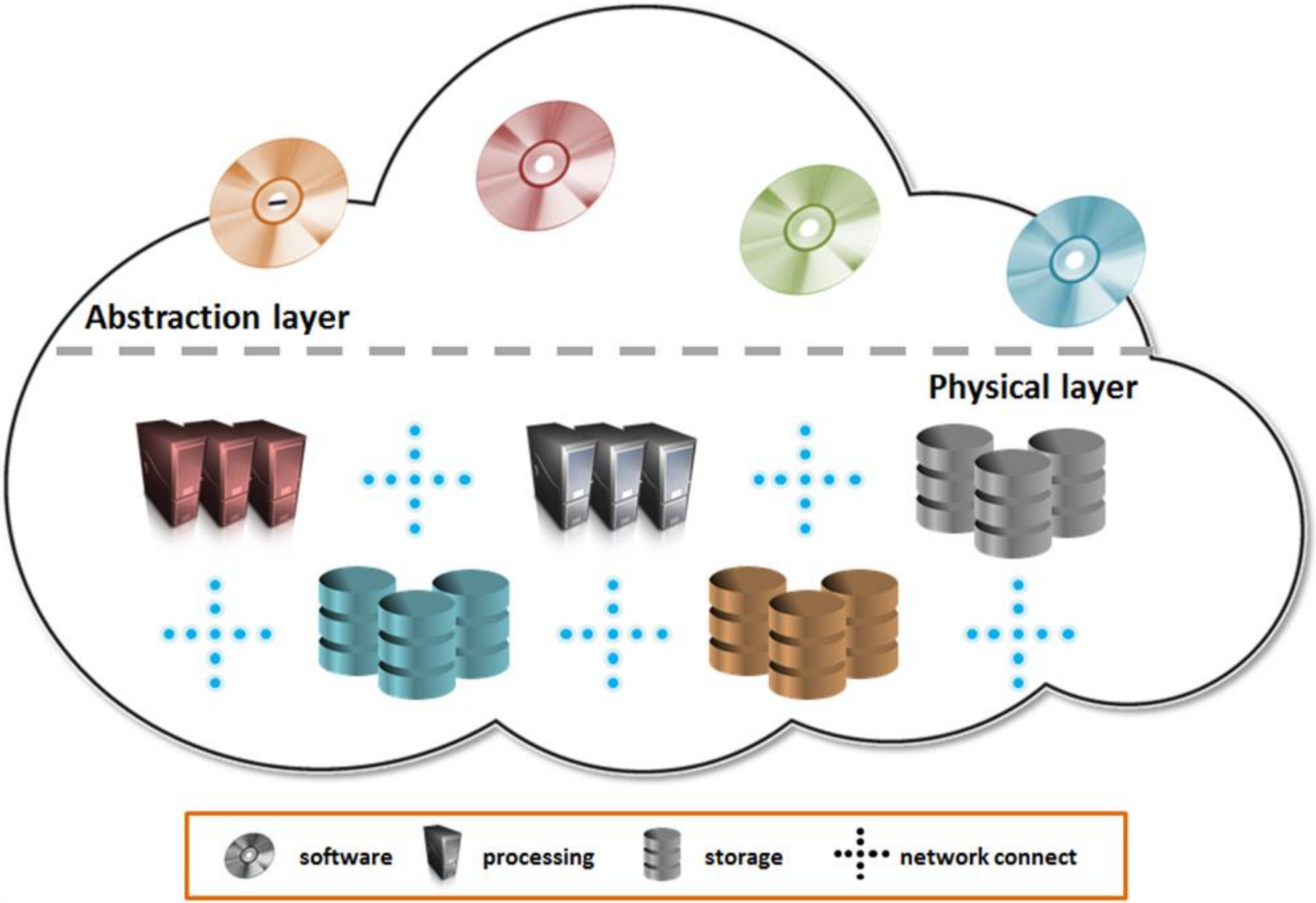
1. **Owned by specific community of consumers from organizations that have shared concerns , missions of security etc.**
2. **owned, managed, and operated by the organization in the community**



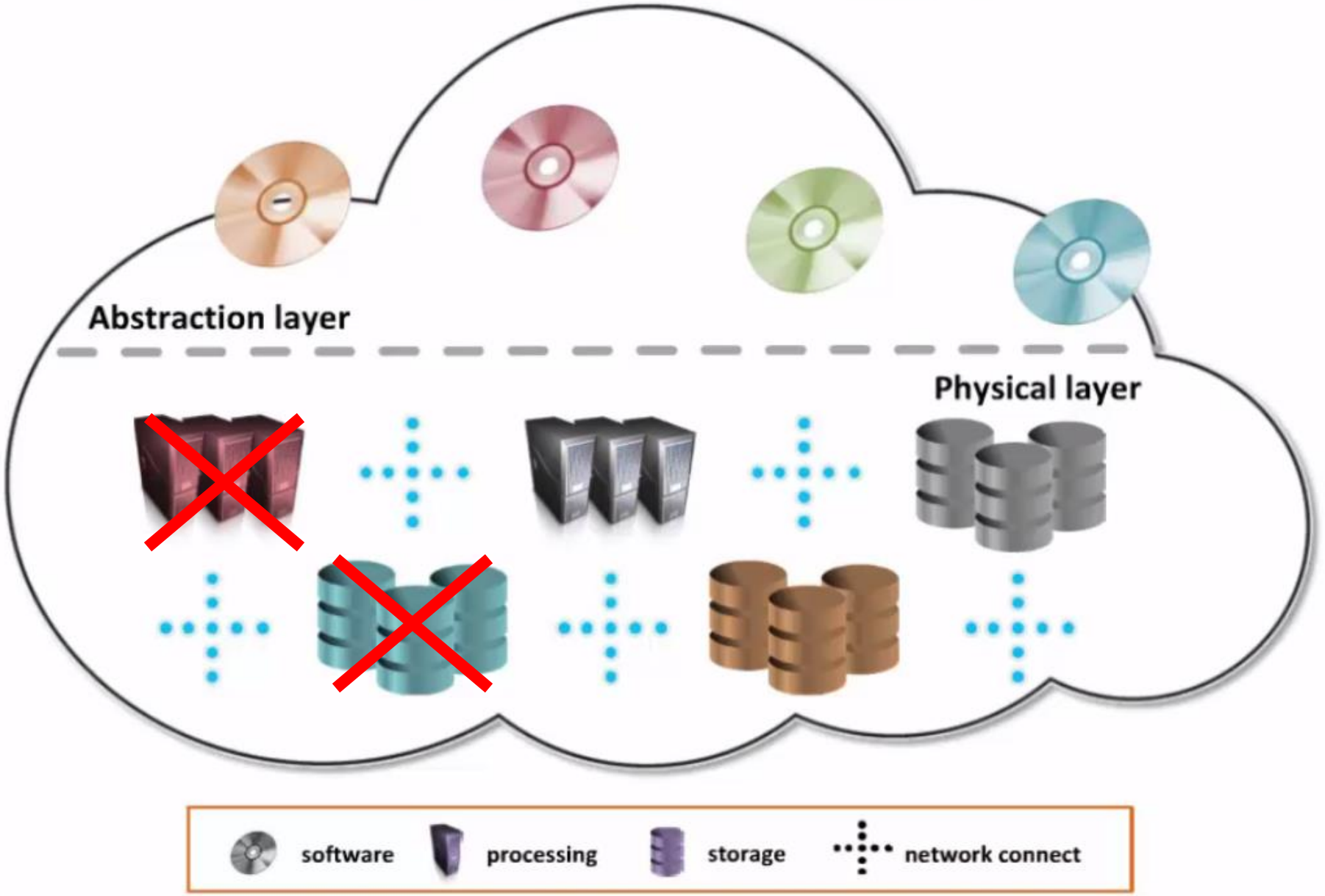
Hybrid cloud infrastructure is

1) **Consists of two or more distinct cloud infrastructures**
2) **Can be private, public, or community based**
3) **Can be proprietary or standardized**
4) **More complex integrated systems**
5) **Subject to implications and constraints**

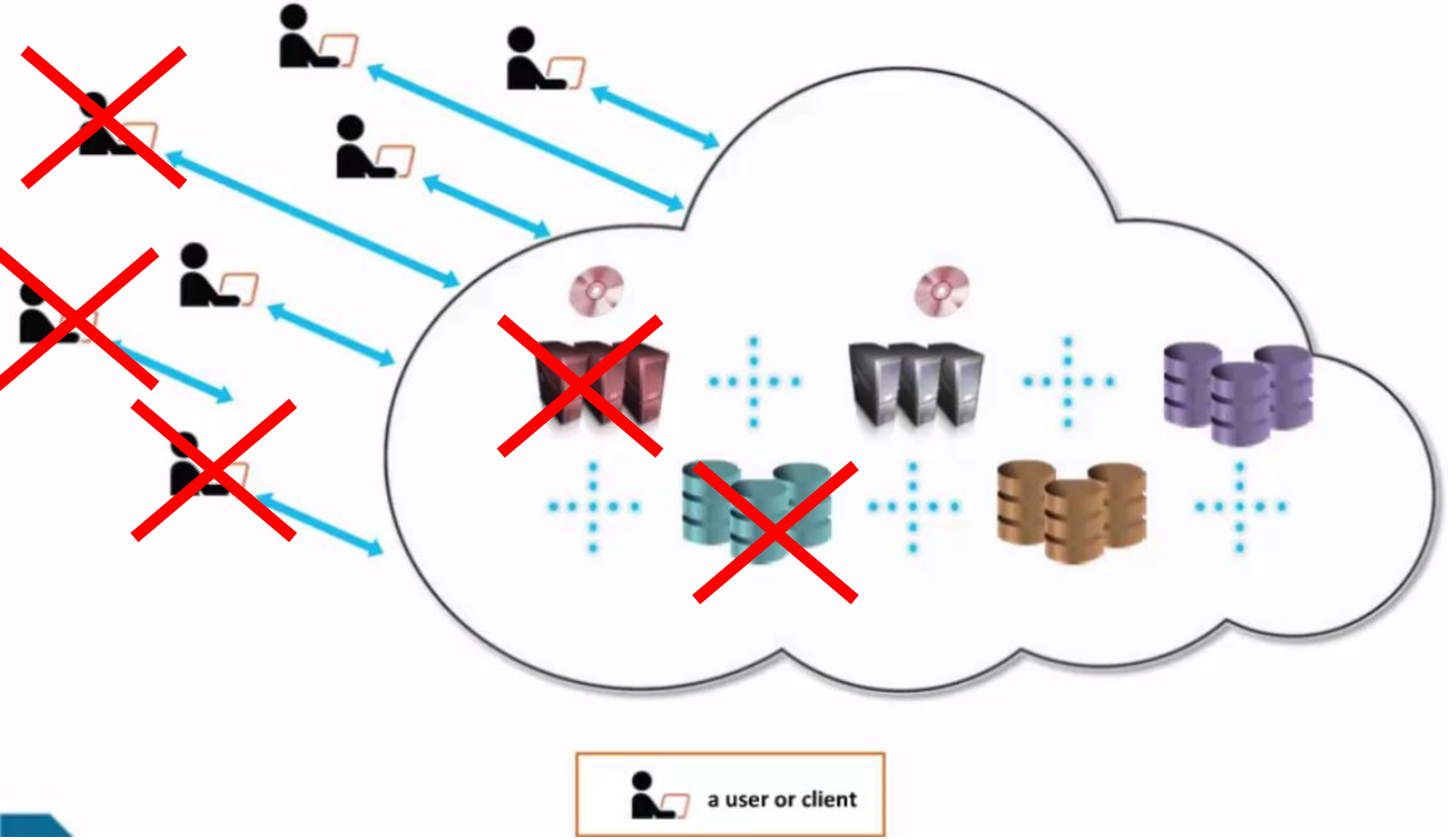
Cloud Infrastructure



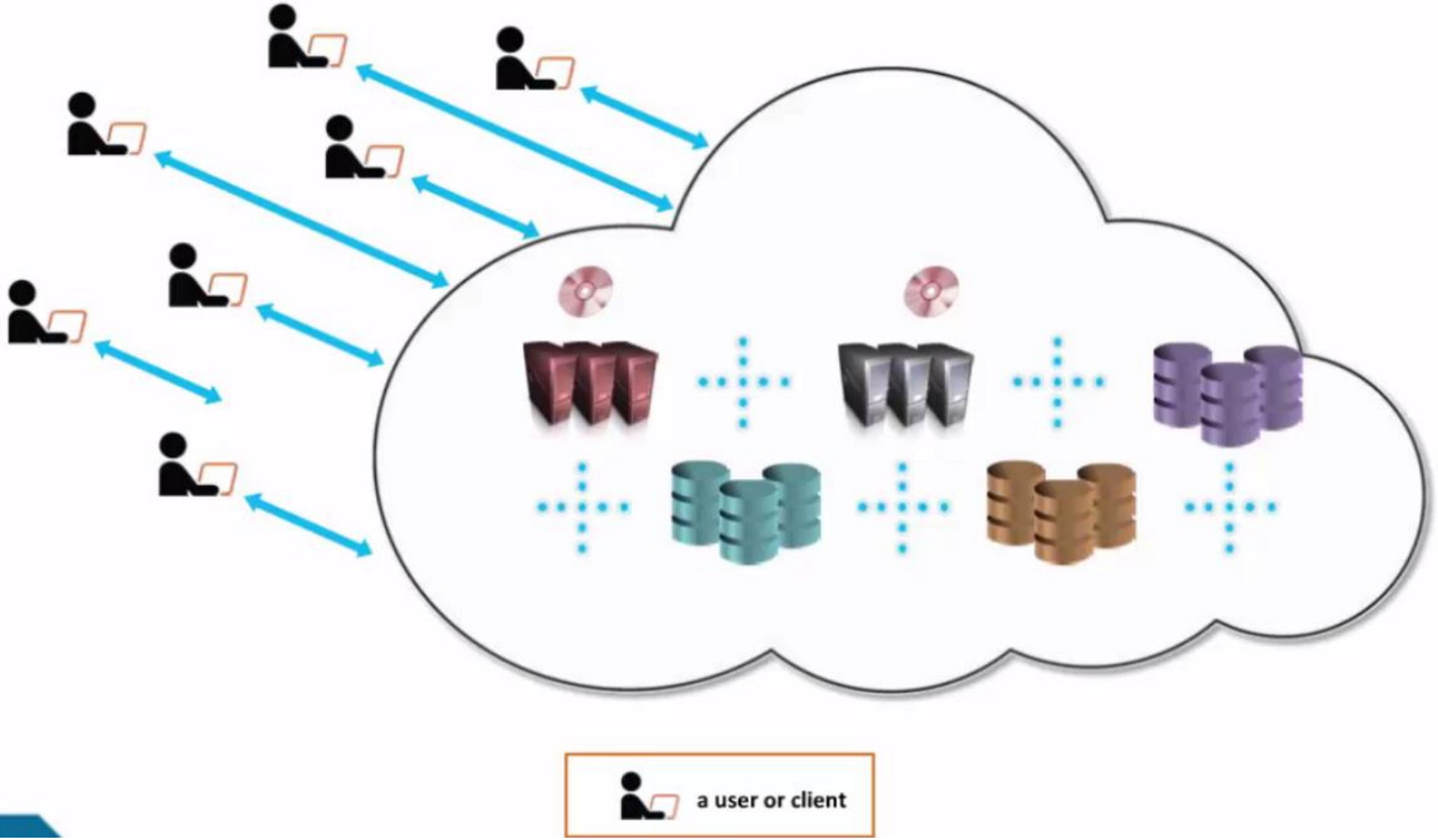
Cloud Infrastructure



General Cloud/Consumer View



General Cloud/Consumer View

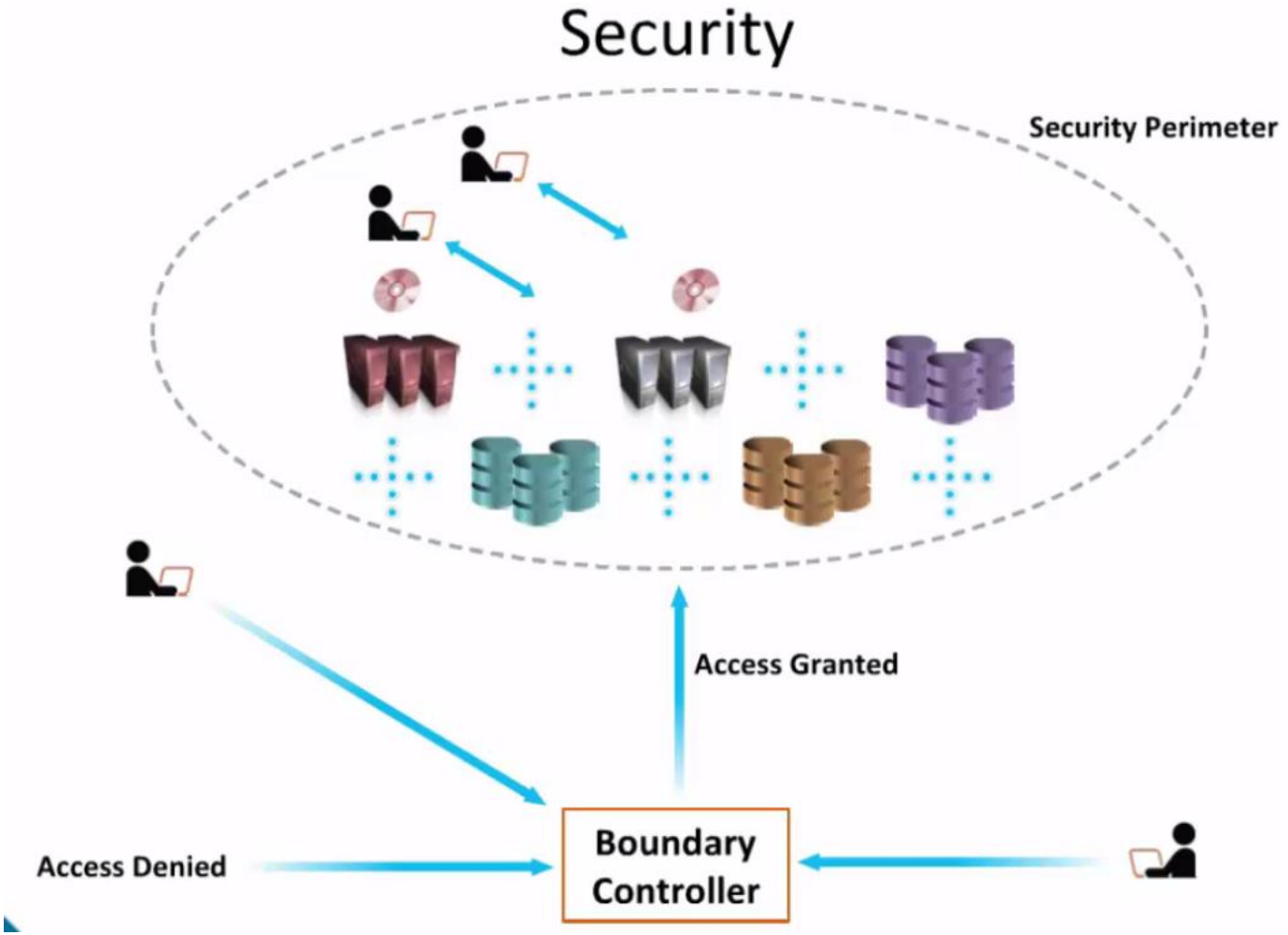


Cloud Security and the Customer

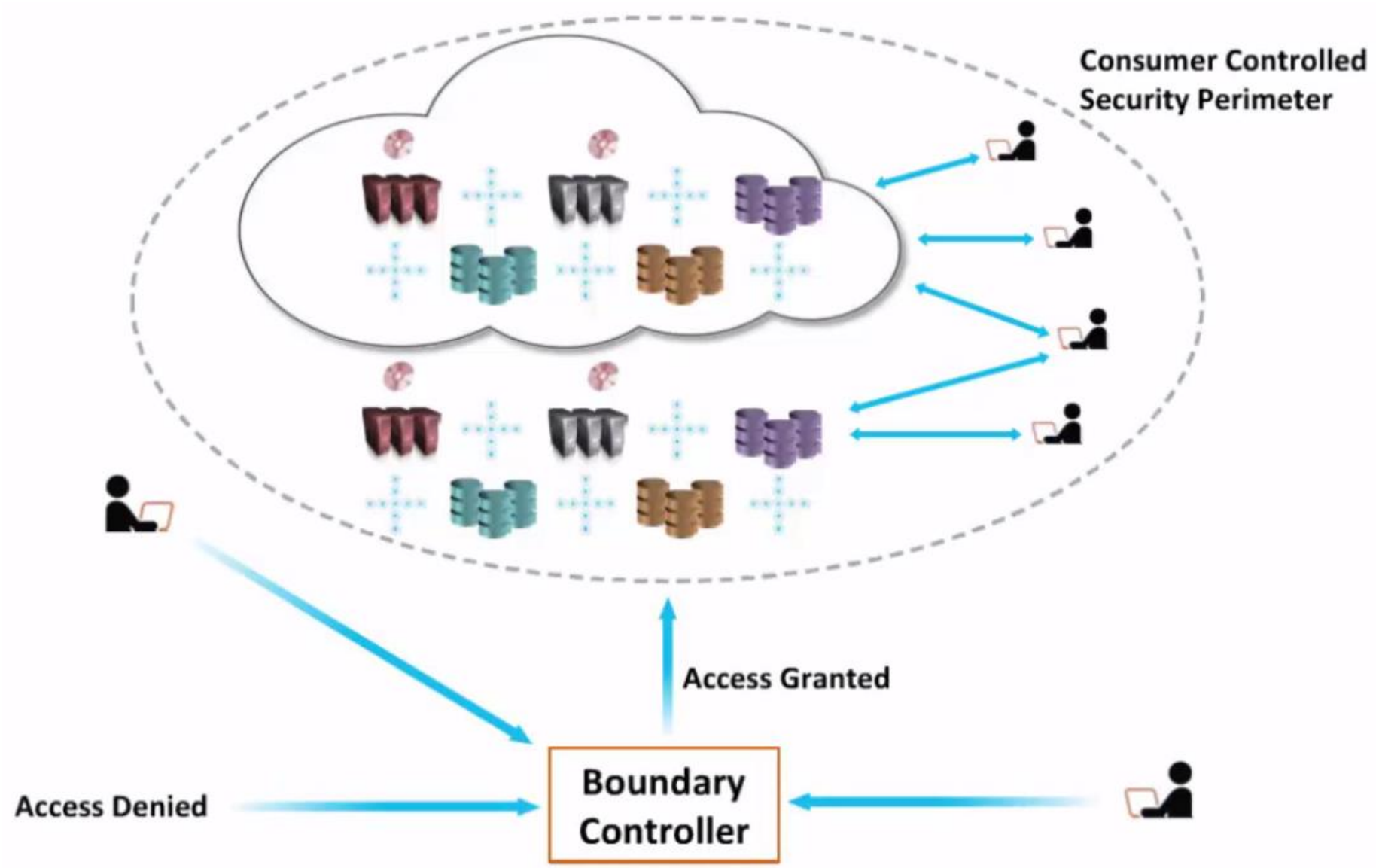
- Assumed the the customer/consumer will relinquish
  - Control
  - Visibility
- Actually it depends:
  - Cloud Model Adapted
  - What is negotiated with the Cloud Provider?

Cloud Security and the Customer

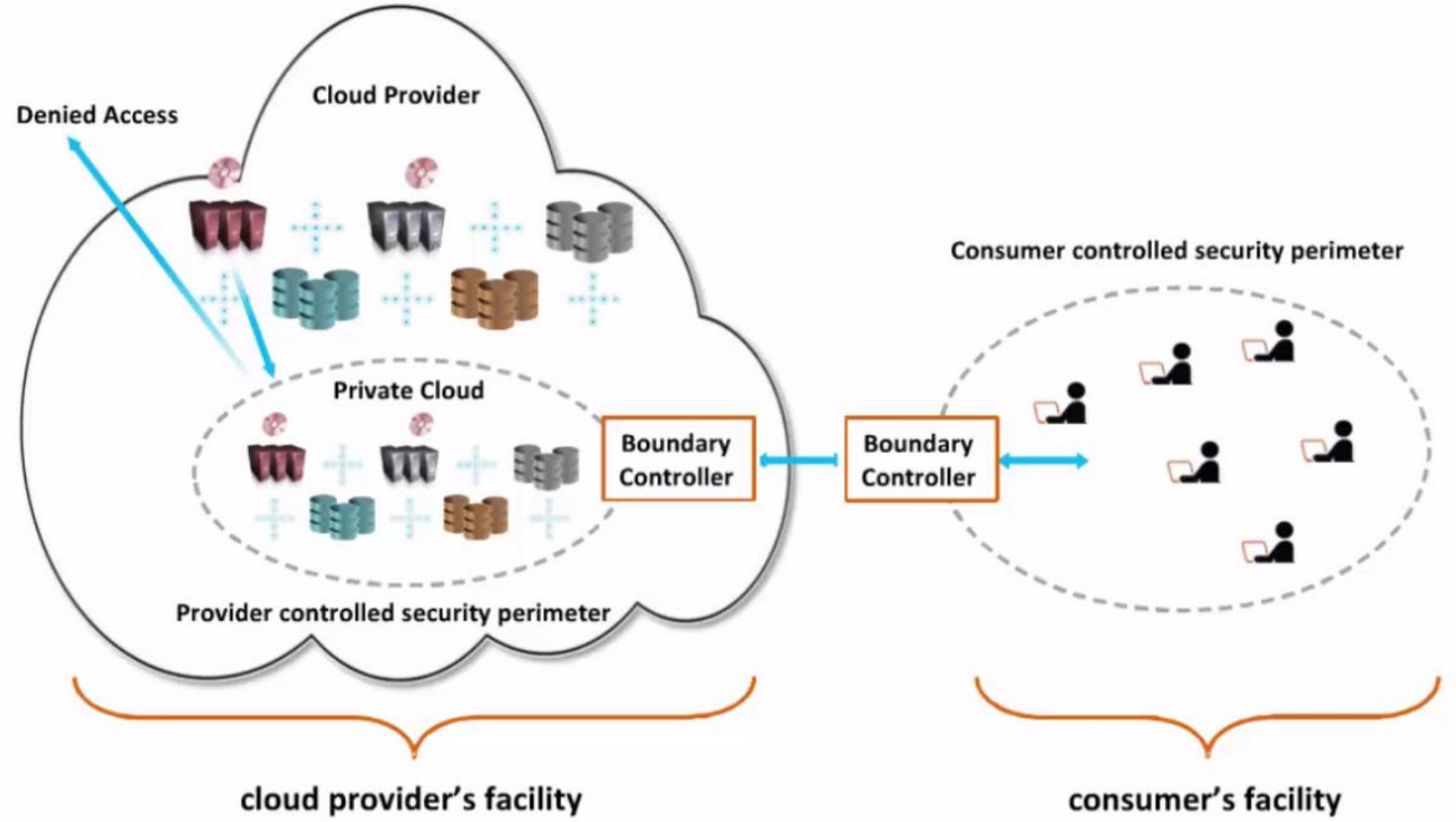
Rights and Control



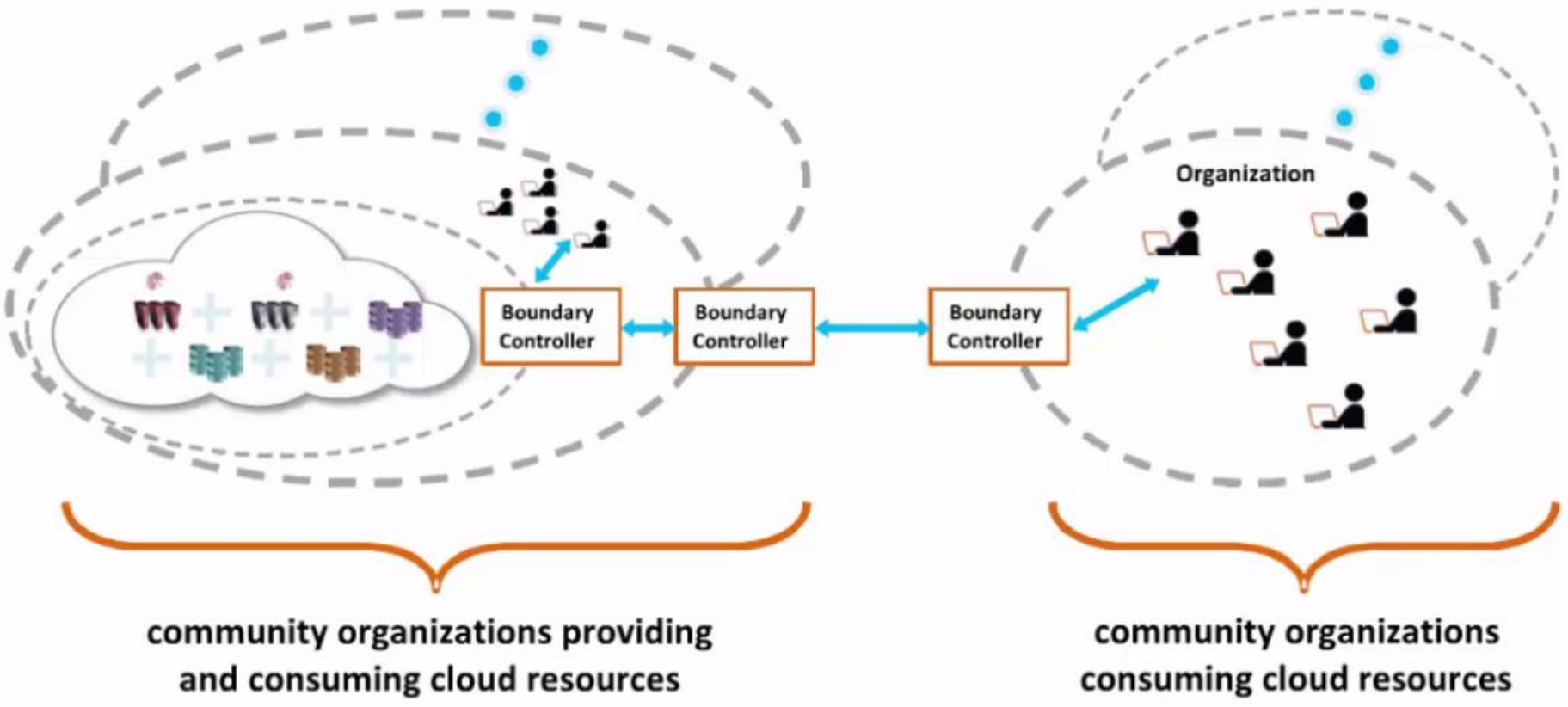
Onsite Private Cloud Scenario



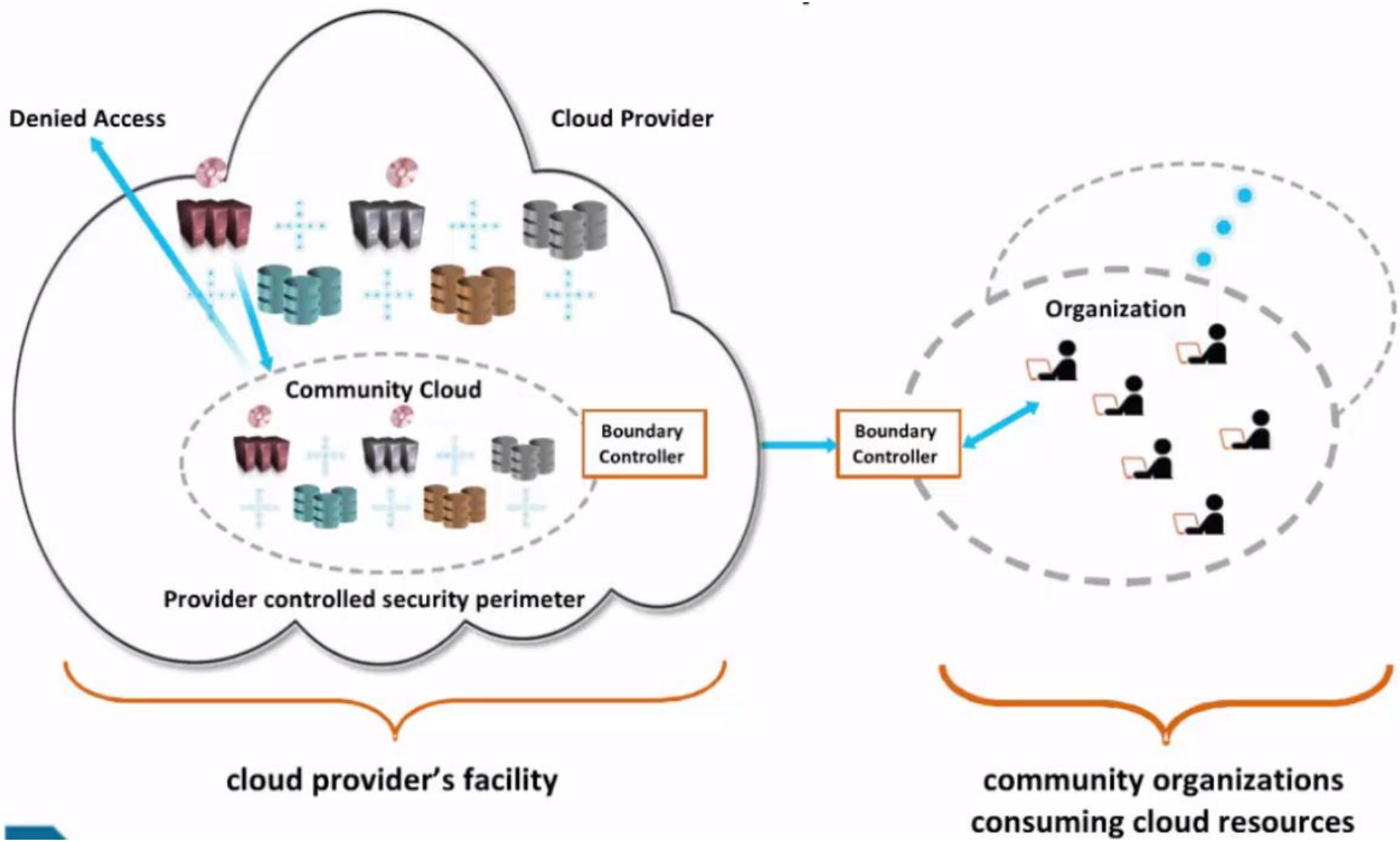
Outsourced Private Cloud Scenario



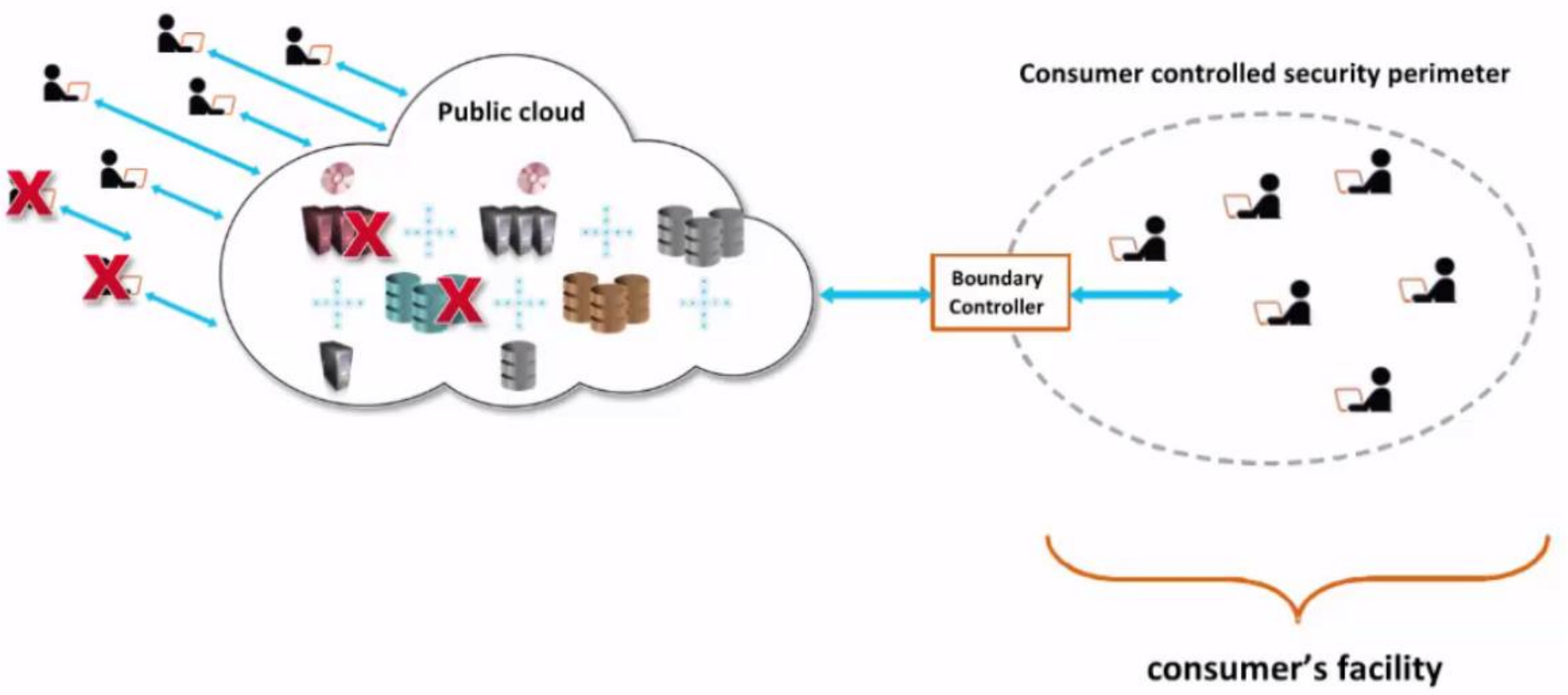
Onsite Community Cloud Scenario



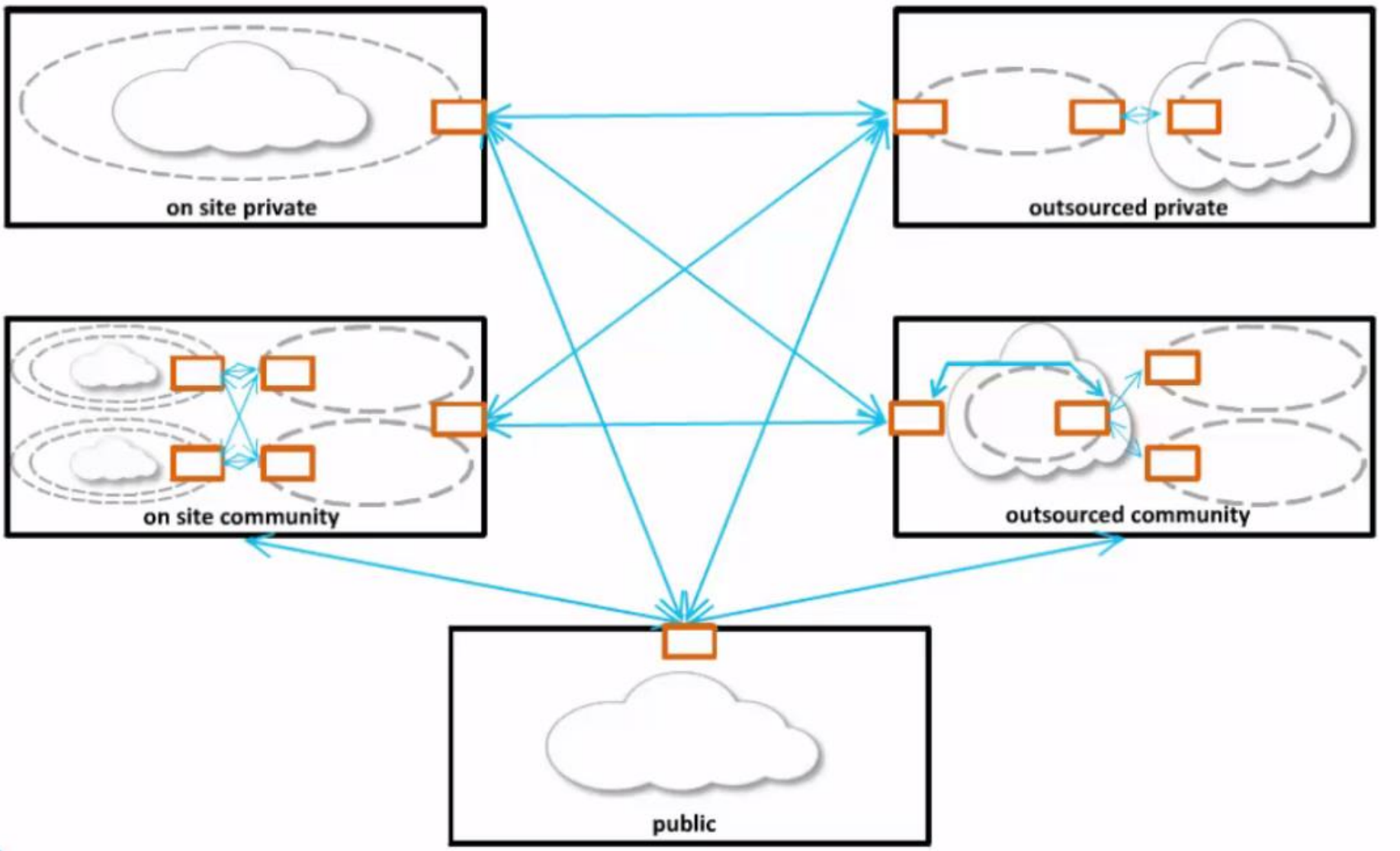
Outsource Community Cloud Scenario



Public Cloud Scenario



Hybrid Cloud Scenario



Hybrid Cloud Possibilities

- Disaster Recovery
- Role Specific Deployment
- Multi Cloud Configurations
- Cloud Bursting

Assumptions

- Network dependency
- Consumer’s IT skills
- Transparent workload assignment
- Risks from multi-tenancy
- Data import/export and performance limitations

Terms of Service

- Service agreement
- Service Level Agreement (SLA)
- Internal agreement
- Memorandum of Understanding (MOU)
- Quality of Service (QoS)
- Provider promises
- Published agreement

Promises

- Availability
- Remedies for failure to perform
- Data preservation
- Legal care of consumer information

Limitations

- Scheduled Outages
- Force Majeure Events
- Service Agreement Changes
- Security
- Service API Changes

Obligations

- Acceptable Use Policies
- Licensed Software
- Timely Payments

Recommendations

- Terminology
- Remedies
- Compliance
- Security, Criticality and Backup
- Negotiated Service Agreement
- Service Agreement Changes

Cloud Computing Implications

- Network Dependency
- IT Skills reduction
- Risks from Multi-tenancy
- Data Import/Export and performance limitations

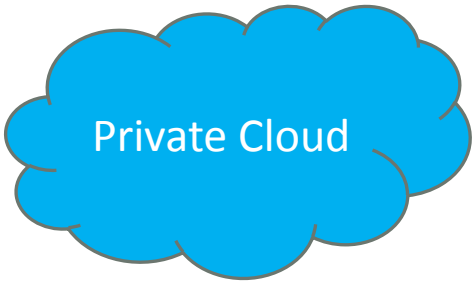
Cloud Service Models

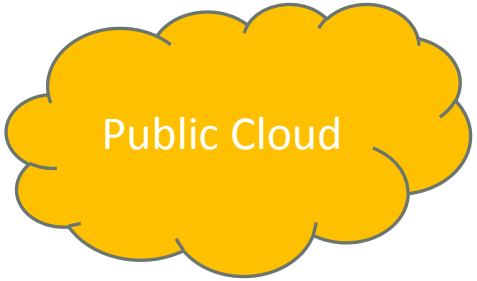
Software as a Service
SaaS

Platform as a Service
PaaS

Infrastructure as a Service
IaaS

Deployment Models





Private cloud the cloud infrastructure is

1) **provisioned for exclusive use by a single organization with**
2) **multiple consumers,**
3) **for example individual business units**
4) **owned, managed, and operated by the organization**

public cloud infrastructure is

1) **provisioned for open use by public**
2) **Owned, managed and operated by a business, government or university**
3) **Mostly in the premises of a cloud provider**

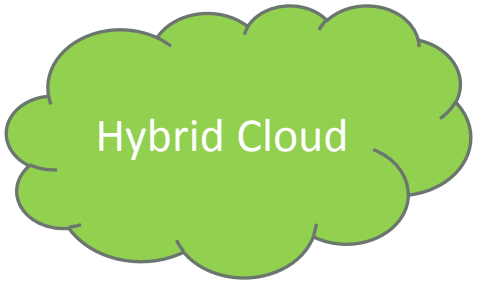
Private or outsourced

Deployment Models

community cloud for use by a community

1. **Owned by specific community of consumers from organizations that have shared concerns , missions of security etc.**
2. **owned, managed, and operated by the organization in the community**

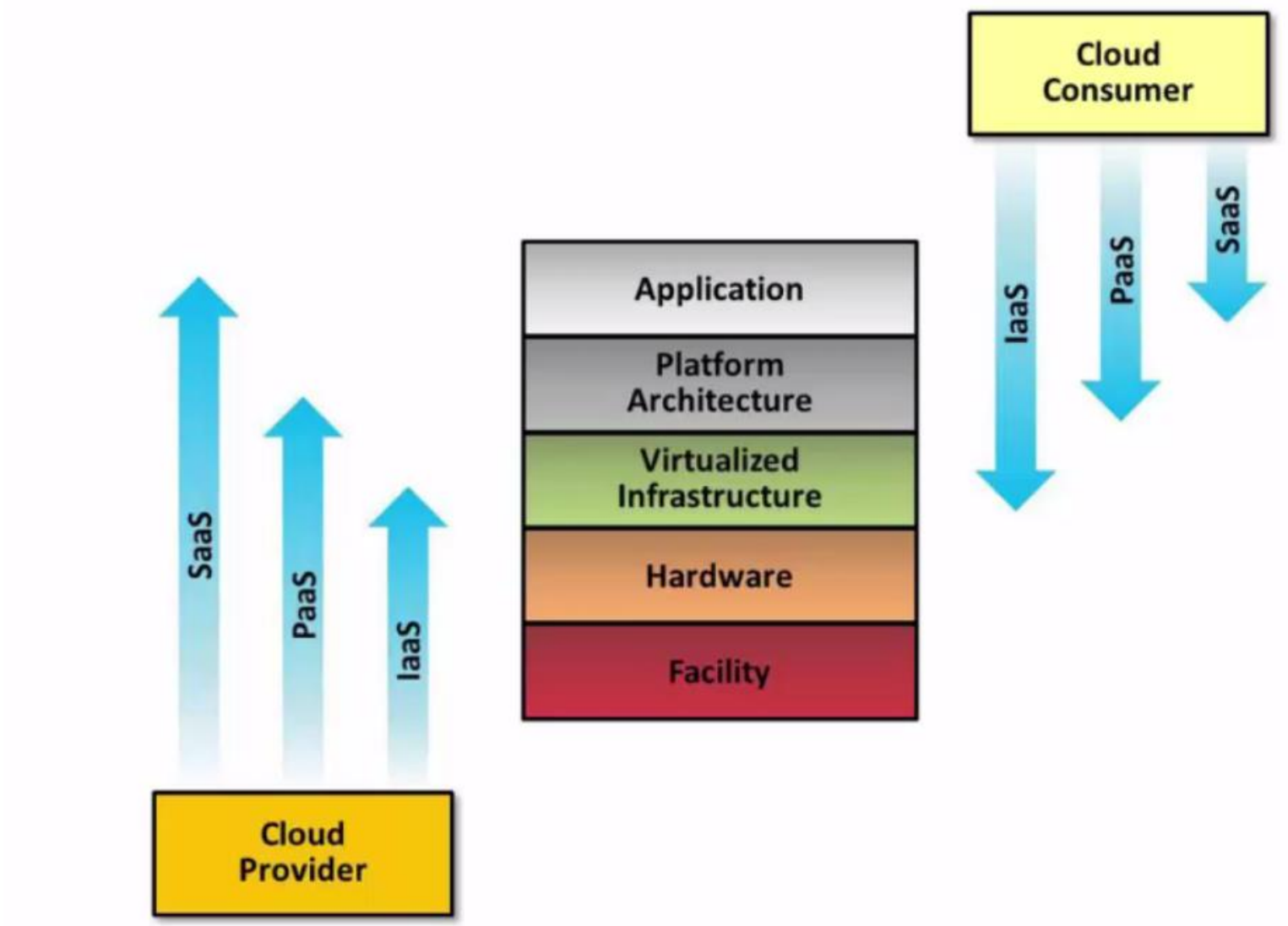
Private or outsourced



Hybrid cloud infrastructure is

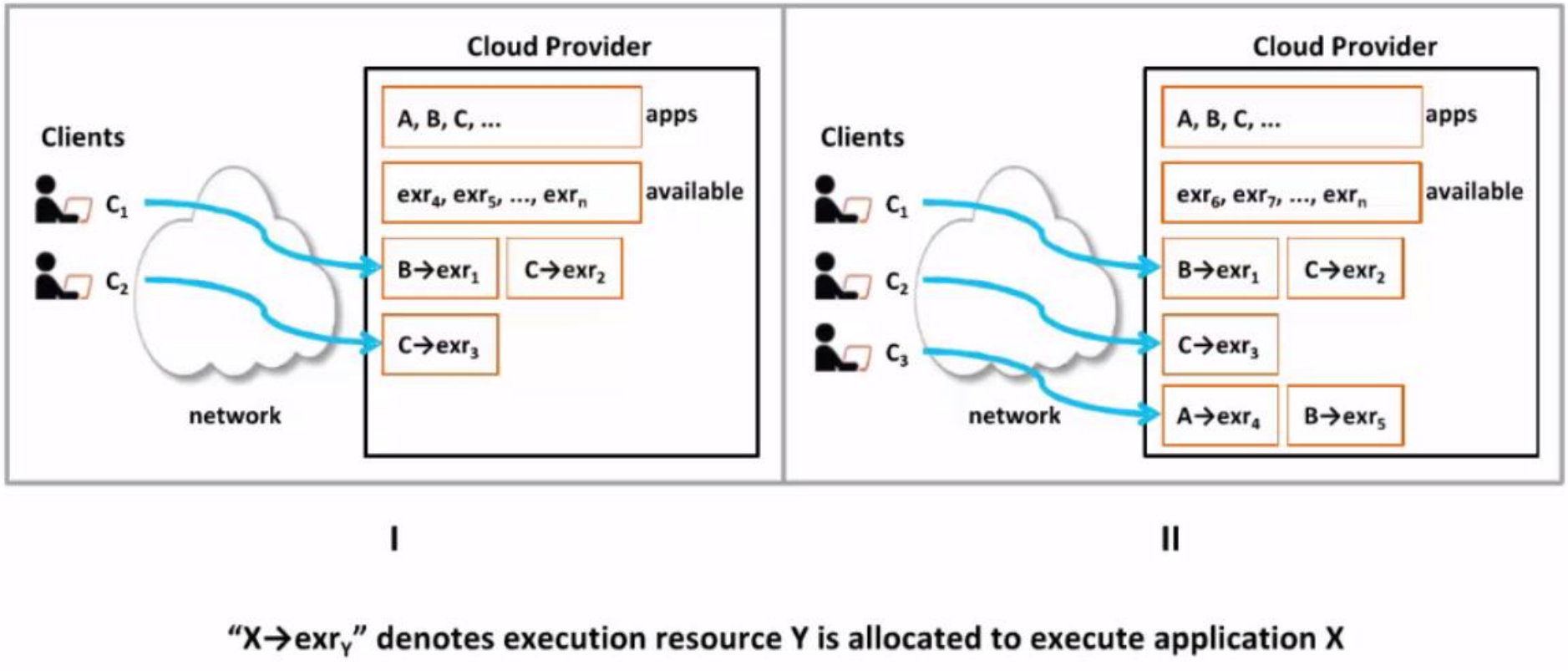
1) **Consists of two or more distinct cloud infrastructures**
2) **Can be private, public, or community based**
3) **Can be proprietary or standardized**
4) **More complex integrated systems**
5) **Subject to implications and constraints**

Scope and Control for the Consumer



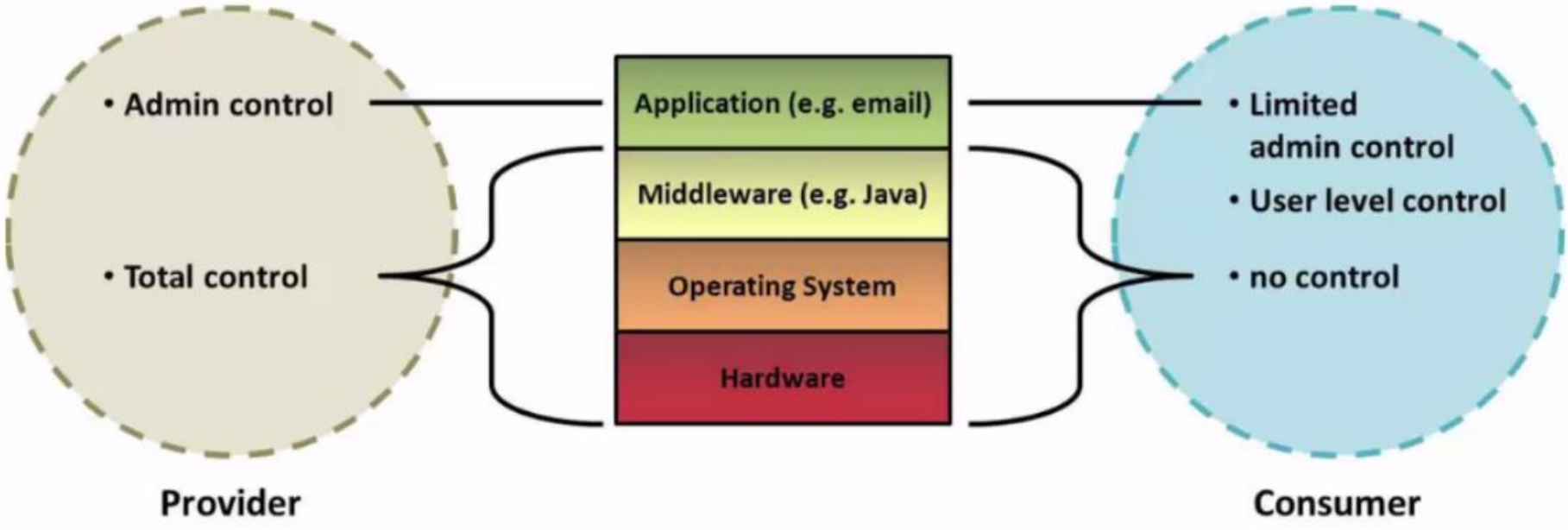
Source: NIST 800-144

SaaS Abstraction Interaction Dynamics



"X→exr$_Y$" denotes execution resource Y is allocated to execute application X

SaaS Software Stack Control



SaaS Benefits

- Reduced Disruption
- Efficient use of Software Licenses
- Centralized Management of Data
- Platform Responsibilities managed by providers
- Up front cost savings

SaaS issues and concerns

- Browser based risks
- Network dependence
- Lack of Portability

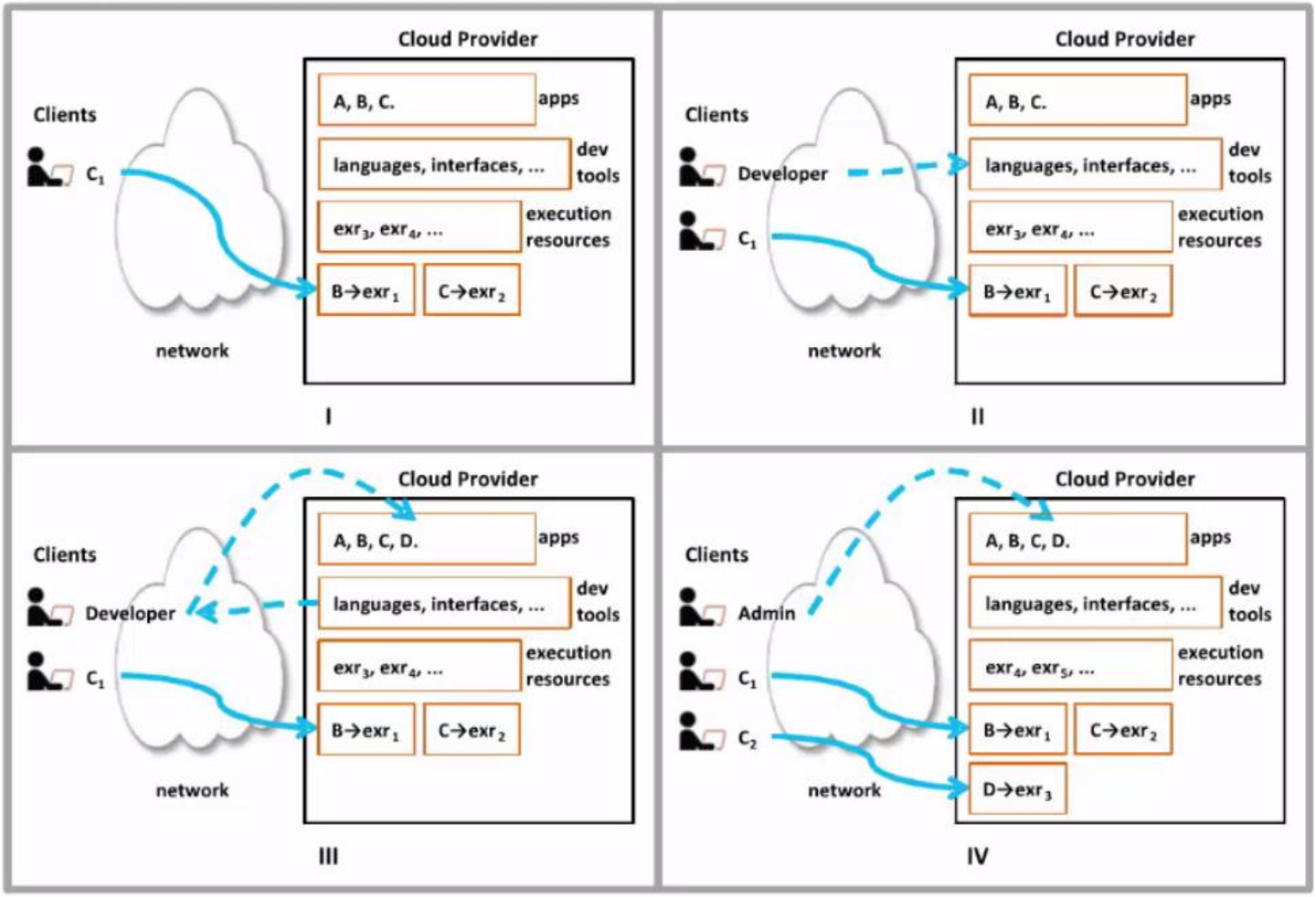
SaaS Application Suitability

- Business Logic
- Collaboration
- Office Productivity
- Software Tools
- Not suitable for any of the following:
  - Real time software
  - Bulk consumer data
  - Critical Software

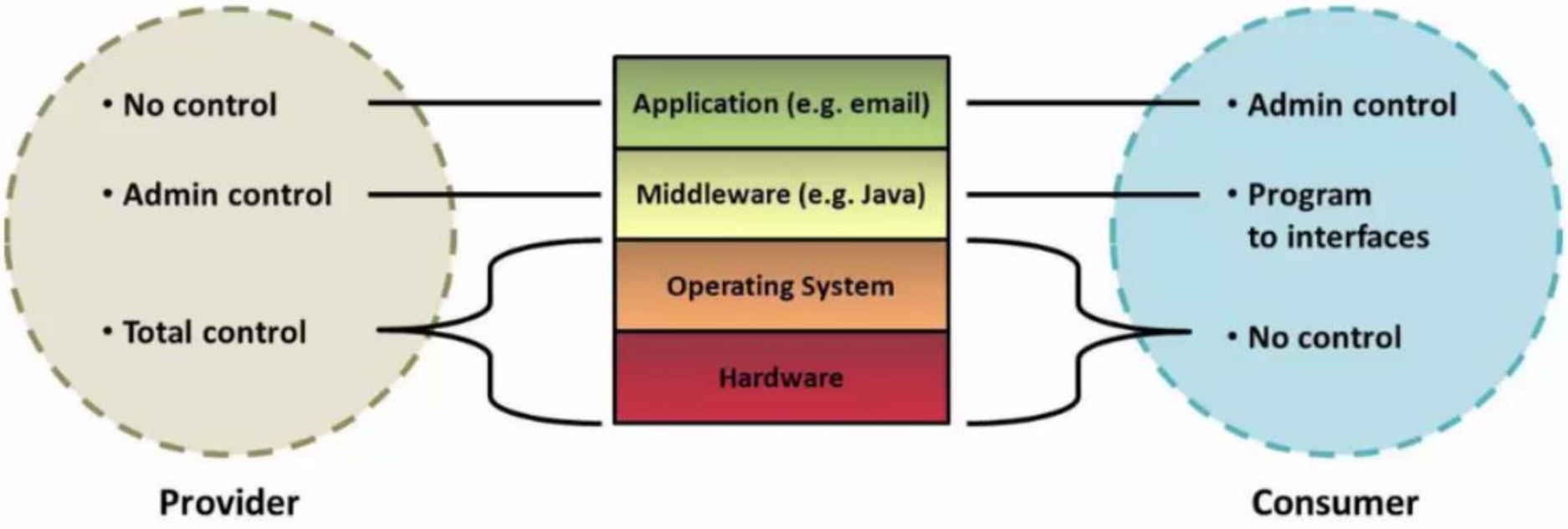
SaaS Recommendations

- Data Protection
- Client Device/Application protection
- Encryption
- Secure data deletion

PaaS Abstract Interaction Dynamics



PaaS Software Stack Control



PaaS Benefits

- Reduced Disruption
- Efficient use of Software Licenses
- Centralized Management of Data
- Platform Responsibilities managed by providers
- Up front cost savings

PaaS Issues and Concerns

- Browser based risks and risk remediation
- Network Dependence
- Isolation vs. Efficiency
- Lack of Portability
- Event based Processor Scheduling
- Security Engineering
- Multiple Languages

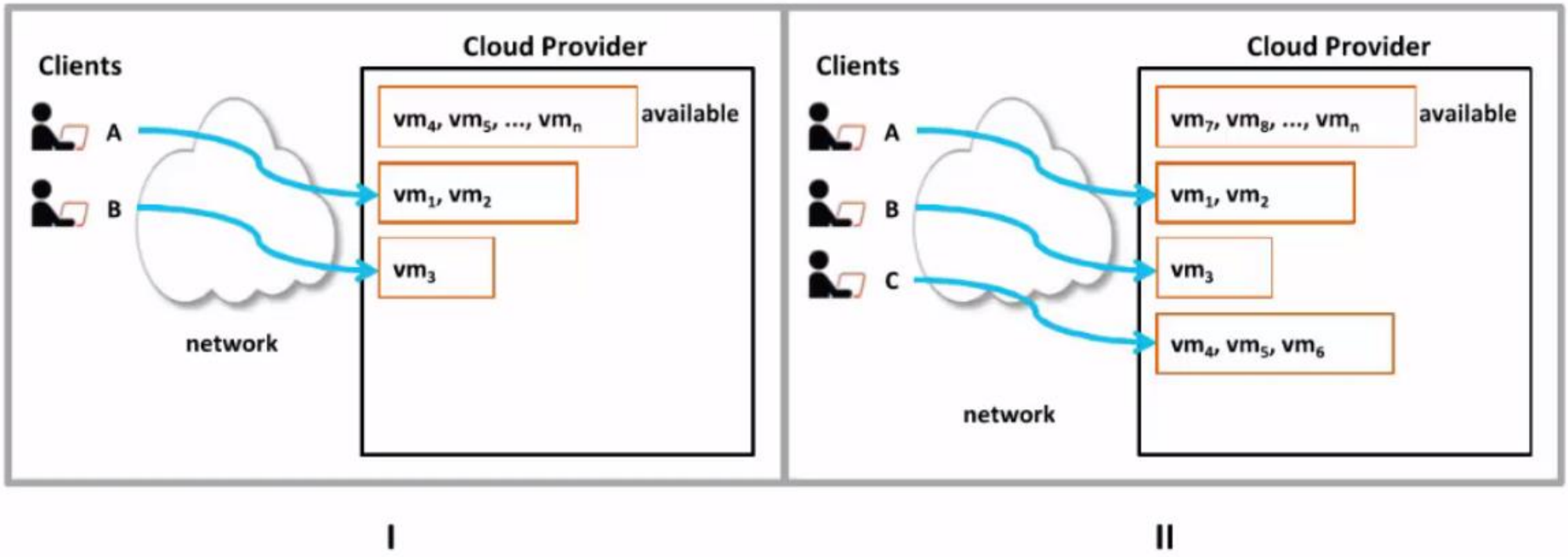
Paas Application Suitability

- PaaS implemented as SaaS
- Application Classes
  - Business Logic
  - Collaboration
  - Office Productivity
  - Software tools

PaaS Recommendations

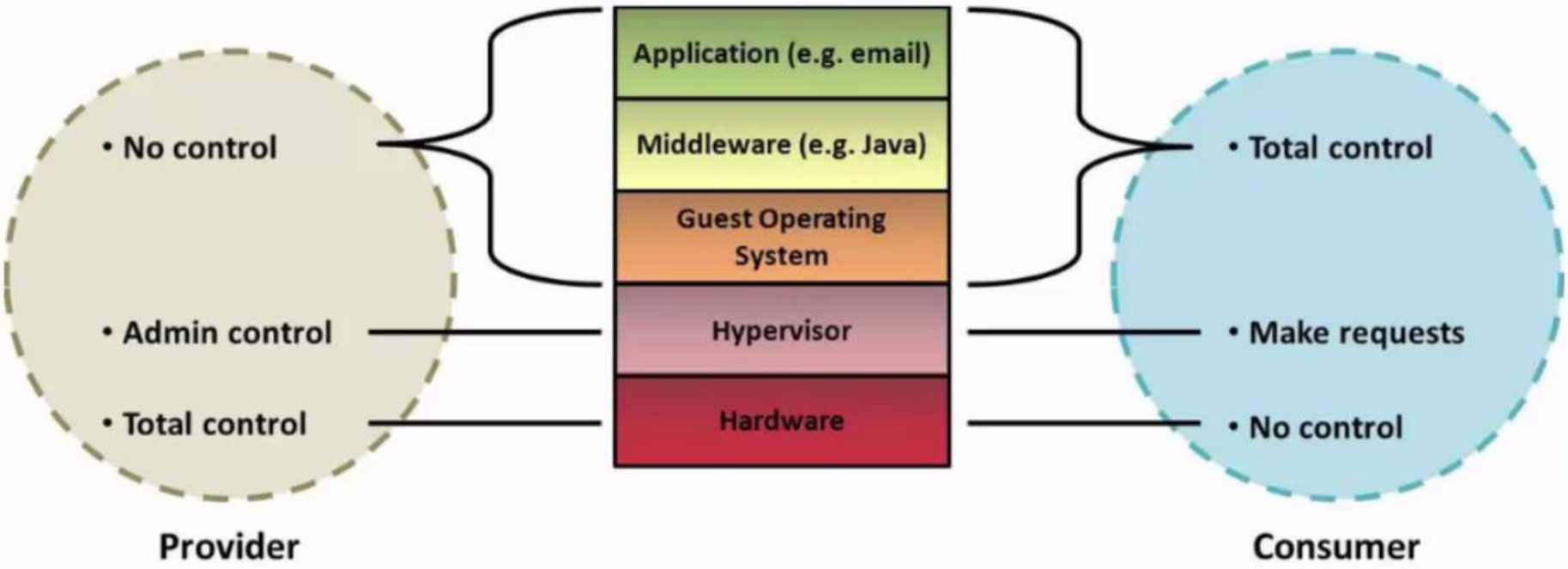
- Generic Interfaces
- Standard Languages and Tools
- Data Access
- Data Protection
- Application Frameworks
- Component Testing
- Security
- Secure Data Deletion

IaaS Abstract Interaction Dynamics

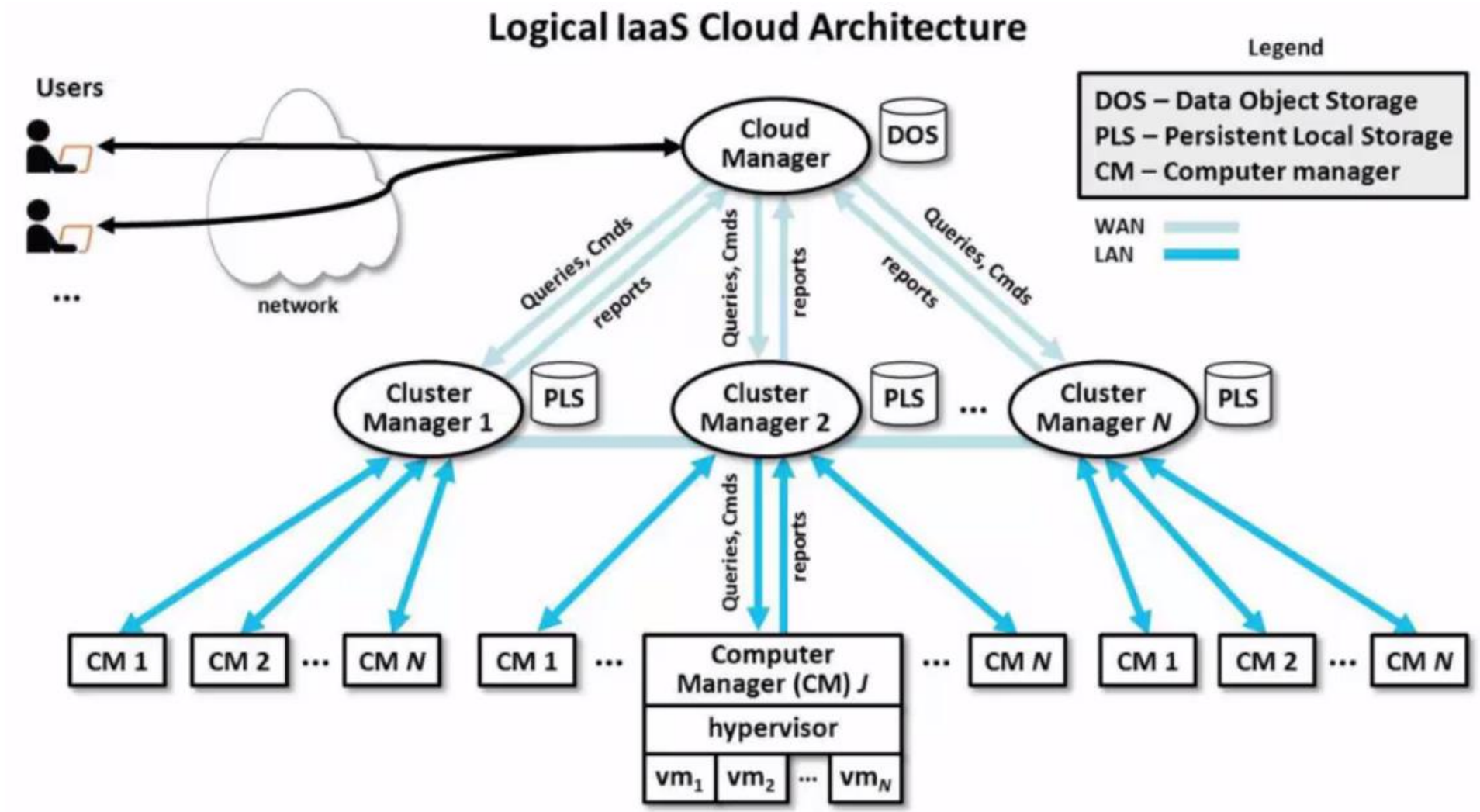


I II

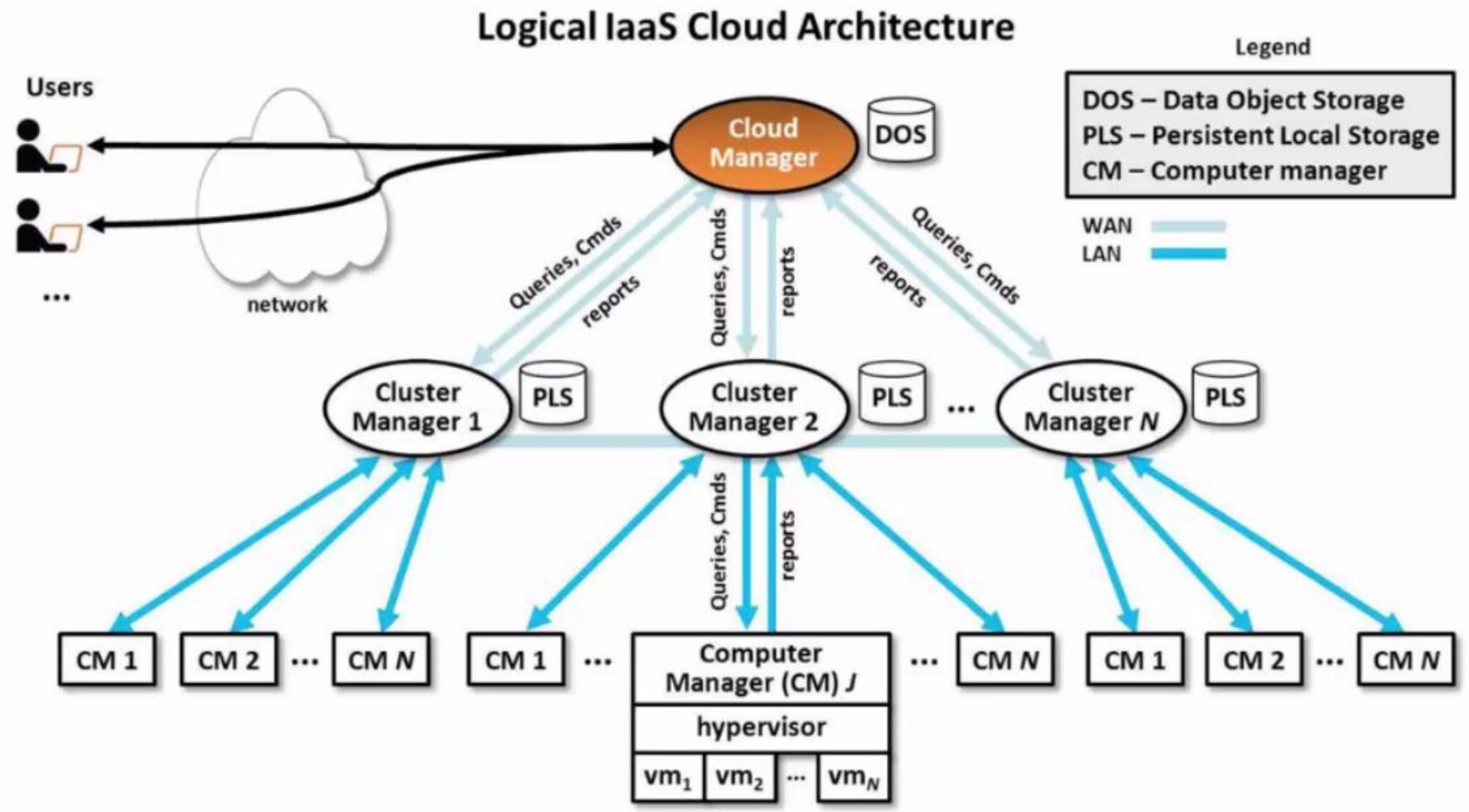
IaaS Software Stack Control



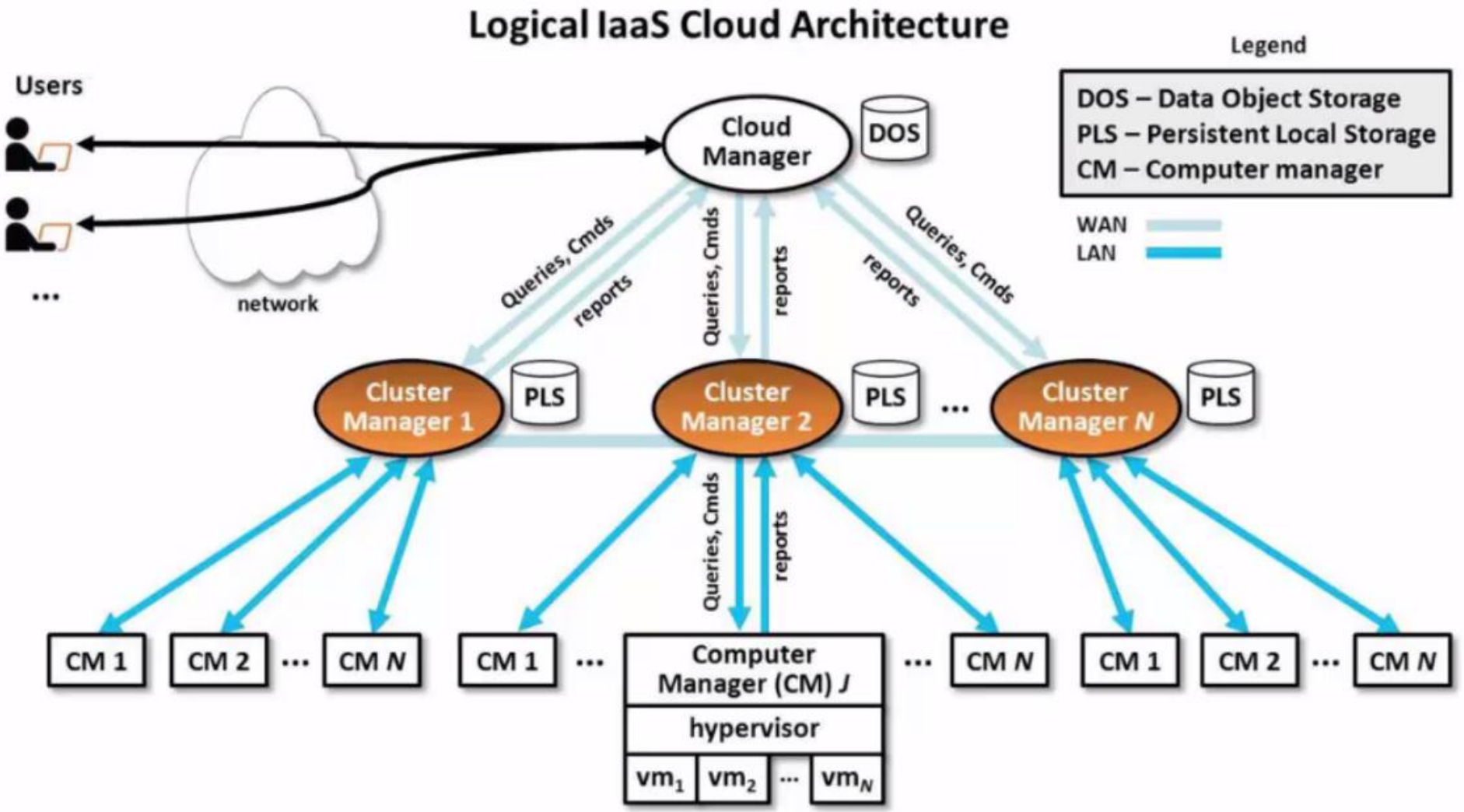
IaaS Operational Overview



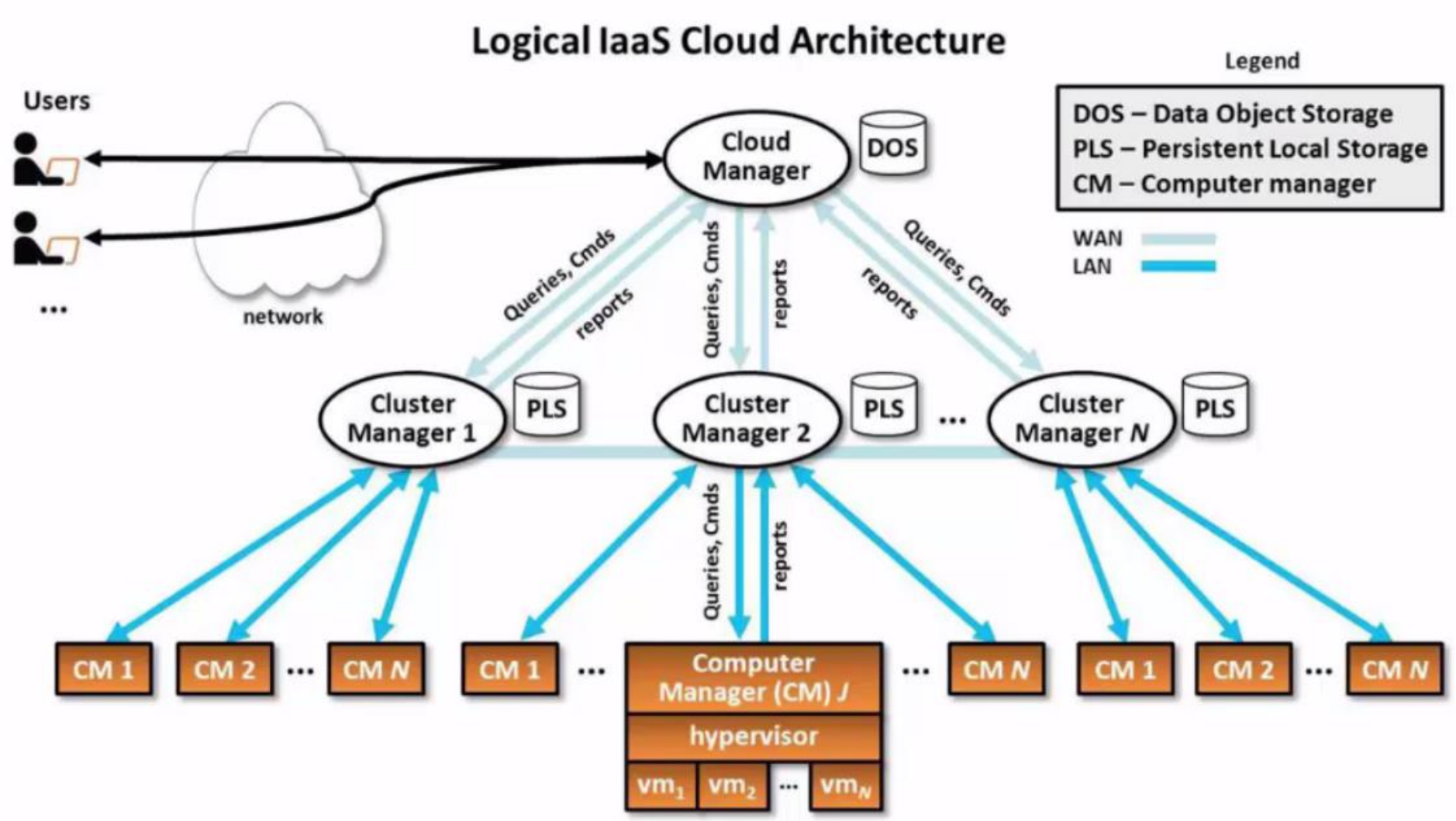
Operation of the Cloud Manager



Operation of the Cluster Managers



Operation of Computer Managers



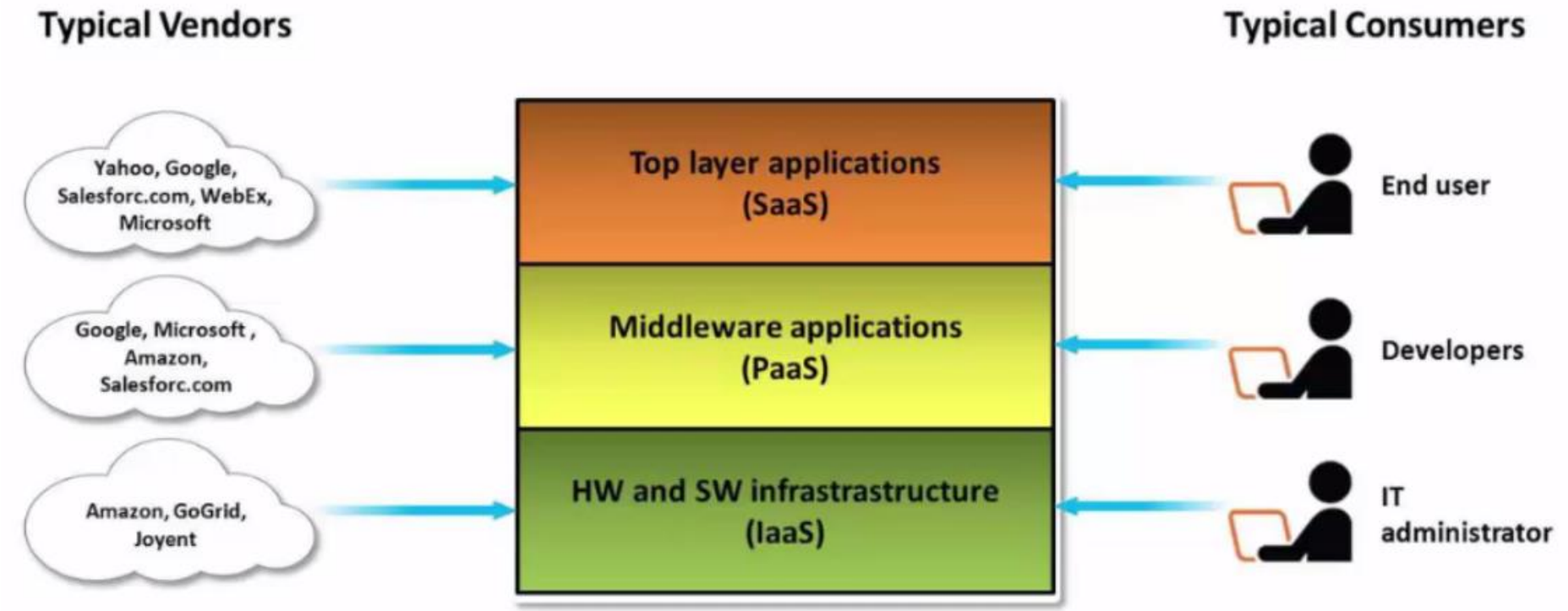
IaaS Issues and Concerns

- Compatibility with legacy security vulnerabilities
- Virtual Machine Sprawls
- Verifying Authencity
- Robustness of VM level isolation
- Features for dynamic network configuration
- Data Erase practices

IaaS Recommendations

- Multi-tenancy
- Data Protection
- Secure Data Deletion
- Administrative Access
- VM Migration
- Virtualization best practices
  - NIST guide to security for full virtualization technologies

Cloud Service Models



SWOT Analysis for Migrating to Cloud

Strengths (internal)	Weaknesses (internal)
Small capital expenses	Latency problems (until next-generation digital transfer technology becomes available)
Easy set-up	Reliability (data loss, code reset during operation)
Easy maintenance	No dedicated personnel
Horizontal scalability (number of instances)	Limited customizability
Vertical scalability (size of instances)	Limited configurability
Redundant data and services	No revenue from support operations
Opportunities (external)	**Threats (external)**
Eco-friendly systems	Data confidentiality, integrity, and availability
Elasticity	Difficulty in cloud-switching interoperability
Conversion of capital expense to operational expense	Legal problems from cross-country data distribution
Quick time to market	No clear downtime agreements or reimbursement policies
Flexible pricing, such as pay per use	No guaranteed return on investment
Tolerance to revenue decreases during crises	Compatibility issues

SWOT Analysis: Migrating to Cloud

Strengths (internal)	Weaknesses (internal)
Small capital expenses	Latency problems (until next-generation digital transfer technology becomes available)
Easy set-up	Reliability (data loss, code reset during operation)
Easy maintenance	No dedicated personnel
Horizontal scalability (number of instances)	Limited customizability
Vertical scalability (size of instances)	Limited configurability
Redundant data and services	No revenue from support operations
Opportunities (external)	**Threats (external)**
Eco-friendly systems	Data confidentiality, integrity, and availability
Elasticity	Difficulty in cloud-switching interoperability
Conversion of capital expense to operational expense	Legal problems from cross-country data distribution
Quick time to market	No clear downtime agreements or reimbursement policies
Flexible pricing, such as pay per use	No guaranteed return on investment
Tolerance to revenue decreases during crises	Compatibility issues

SWOT Analysis: Migrating to Cloud

Strengths (internal)	Weaknesses (internal)
Small capital expenses	Latency problems (until next-generation digital transfer technology becomes available)
Easy set-up	Reliability (data loss, code reset during operation)
Easy maintenance	No dedicated personnel
Horizontal scalability (number of instances)	Limited customizability
Vertical scalability (size of instances)	Limited configurability
Redundant data and services	No revenue from support operations
Opportunities (external)	**Threats (external)**
Eco-friendly systems	Data confidentiality, integrity, and availability
Elasticity	Difficulty in cloud-switching interoperability
Conversion of capital expense to operational expense	Legal problems from cross-country data distribution
Quick time to market	No clear downtime agreements or reimbursement policies
Flexible pricing, such as pay per use	No guaranteed return on investment
Tolerance to revenue decreases during crises	Compatibility issues

SWOT Analysis: Migrating to Cloud

Strengths (internal)	Weaknesses (internal)
Small capital expenses	Latency problems (until next-generation digital transfer technology becomes available)
Easy set-up	Reliability (data loss, code reset during operation)
Easy maintenance	No dedicated personnel
Horizontal scalability (number of instances)	Limited customizability
Vertical scalability (size of instances)	Limited configurability
Redundant data and services	No revenue from support operations
Opportunities (external)	**Threats (external)**
Eco-friendly systems	Data confidentiality, integrity, and availability
Elasticity	Difficulty in cloud-switching interoperability
Conversion of capital expense to operational expense	Legal problems from cross-country data distribution
Quick time to market	No clear downtime agreements or reimbursement policies
Flexible pricing, such as pay per use	No guaranteed return on investment
Tolerance to revenue decreases during crises	Compatibility issues

SWOT Analysis: Migrating to Cloud

Strengths (internal)	Weaknesses (internal)
Small capital expenses	Latency problems (until next-generation digital transfer technology becomes available)
Easy set-up	Reliability (data loss, code reset during operation)
Easy maintenance	No dedicated personnel
Horizontal scalability (number of instances)	Limited customizability
Vertical scalability (size of instances)	Limited configurability
Redundant data and services	No revenue from support operations
Opportunities (external)	**Threats (external)**
Eco-friendly systems	Data confidentiality, integrity, and availability
Elasticity	Difficulty in cloud-switching interoperability
Conversion of capital expense to operational expense	Legal problems from cross-country data distribution
Quick time to market	No clear downtime agreements or reimbursement policies
Flexible pricing, such as pay per use	No guaranteed return on investment
Tolerance to revenue decreases during crises	Compatibility issues

General Value Proposition

- Technical
- Human
- Relational

SaaS Value Proposition

- Typical Customers
  - Organizations
  - End Users
  - Administrators
- Consumer value
- Usage fees

PaaS Value Proposition

- Typical Consumers
  - Application developers
  - Application testers
  - Application deployers
  - Application administrators
  - Application end users
- Consumer Value
- Usage Fees

IaaS Value Proposition

- Typical Consumers
  - Small and Medium Business
  - Enterprises
  - Startups
  - Communities
- Consumer Value
- Usage Fees

General Cloud Computing Risks

- Complexity

General Cloud Computing Risks

- Complexity
- Exposure of Critical Data

General Cloud Computing Risks

- Complexity
- Exposure of Critical Data
- Technical and Economic Concerns

Risks: Computing Performance

- Latency
  - Not under control of Consumer
  - Not under the control of Cloud Provider
  - Decision to determine which applications will be cloud based

Risks: Computing Performance

- Offline Data synchronization
  - When Consumer is offline (Requires version control)

Risks: Computing Performance

- Scalable Programming
  - For high performance computing needs for data analytics
  - For scientific studies etc.
  - Many of the above environments requires a careful examination of cloud provider environment

Risks: Computing Performance

- Data Storage Management poses challenges
  - Provisioning
  - Local restriction
  - Erasure verification
  - Secure disposal
  - Access control

Risks: Cloud Reliability

- Reliability
  - Hardware and Software
  - Cloud providers personnel
  - Connectivity
  - Consumer's personnel
- Measurement
  - Composition
  - Environment
  - Intractable

Risks: Network Dependence

- Continuous Service
- Complexity
  - Health
  - Contention
  - Force Majeure
- Denial of Service Attacks

Risks: Cloud Provider Outages

- Inevitable downtime
  - Attacks
  - Errors
  - Disasters
- Outage Frequency
- Frequency
- Resiliency

Risks: Safety Critical Processing

- Loss of life or property
- Regulated by government
- Pedigree

Risks: Compliance

- Lack of visibility
- Physical Data location
- Regulation
- Jurisdiction
- Forensics

Risks: Information Security

- Risks of unintended disclosure
- Data Privacy
- System Integrity
- Multi-Tenancy
- Browsers

Value/Risk: Open Source Software

- Easy deployable
- Interoperability and Standards
- Openness = vulnerability
- Loss of control
- Licensing risks

Up front costs

$$C_{u(SaaS)} = N \cdot C_{SaaS\_sub} + C_{in} + C_{ut} + C_o$$

$$C_{u(in-house)} = C_d + C_{ps} + C_{in} + C_{ut} + C_h + C_o$$

$$C_{u(IaaS)} = C_d + C_{ps} + C_{in} + C_{ut} + \sum_{i=1}^{S} U_i \cdot F_i + C_o$$

Key	
Symbol	Cost
C_d	custom development
C_h	hardware and middleware
C_{in}	integration
C_{net}	networking infrastructure
C_o	ongoing operations
C_{ps}	professional services
C_{SaaS_sub}	annual SaaS subscription
C_{ut}	user training
F_i	usage fee
N	number of client instances
S	number of server instances
U_i	level of usage

Operational costs

$$C_{o(SaaS)} = C_{ic}$$

$$C_{o(in-house)} = C_{ic} + C_{adm} + C_{pow} + C_{floor}$$

$$C_{o(IaaS)} = C_{ic}$$

Key	
Symbol	Cost
C_{adm}	administrator labor
C_{floor}	floor space
C_{ic}	Internet connection
C_{net}	networking infrastructure
C_{o}	ongoing operations
C_{pow}	power
C_{sec}	security

Annual Disinvestment Costs

$$C_{ad(SaaS)} = N \cdot C_{SaaS\_sub} + C_{a\_ps} + C_{a\_cust}$$

$$C_{ad(in-house)} = C_{a\_smain} + C_{a\_hmain} + C_{a\_ps} + C_{a\_cust}$$

$$C_{ad(IaaS)} + C_{a\_smain} C_{a\_ps} + C_{a\_cust} + \sum_{i+1}^{S} U_i \cdot F_i + C_o$$

Key	
Symbol	**Cost**
C_{a_cust}	customer support
C_{ad}	annual divestment
C_{a_hmain}	hardware maintenance
C_{a_ps}	professional support
C_{a_smain}	software maintenance
C_o	ongoing operations
C_{SaaS_sub}	annual SaaS subscription
F_i	usage fee
N	Number of client instances
U_i	level of usage

Total Cost of Ownership

$$TCO = C_u + \sum_{i=2}^{n} (C_{ad} + C_o)$$

Key	
Symbol	Cost
C_{ad}	annual divestment
C_o	ongoing operations
C_u	Upfront
n	number of years

Selecting an IaaS provider

- Pricing plan
- Average monthly cost
- Service level agreement (SLA)
- Number of datacenters
- Certifications
- Scale up
- Scale out
- Support
- Monitoring
- APIs
- Free tier
- Supported operating systems
- Number of instance types
- Cost of outbound data transfer
- Cost of inbound data transfer

Source: Rodrigues

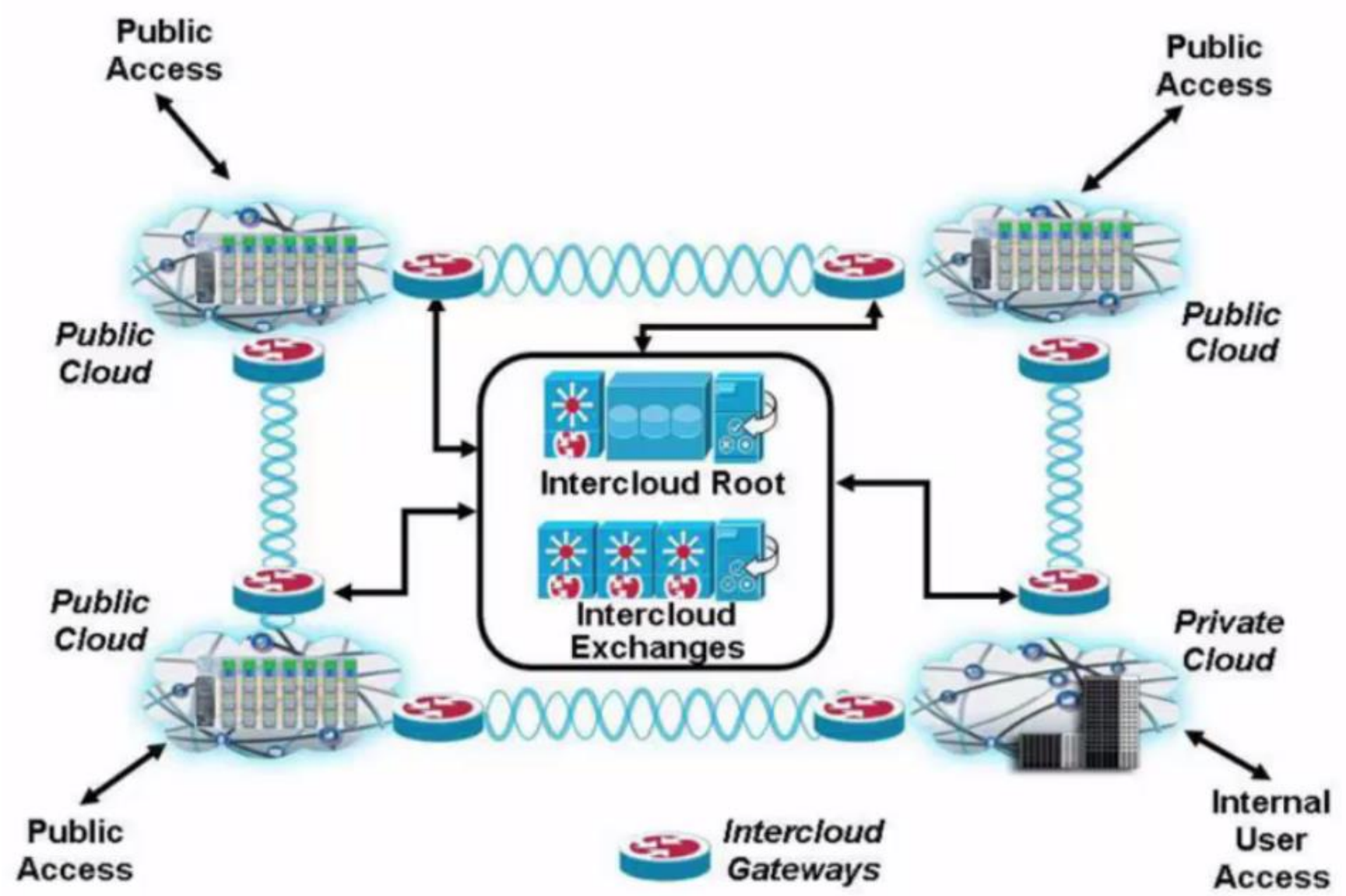
IEEE P2301 Standard

- Portability and Interoperability Standards
- Standards based choices
- Different Cloud personalities

IEEE P2302 Standard

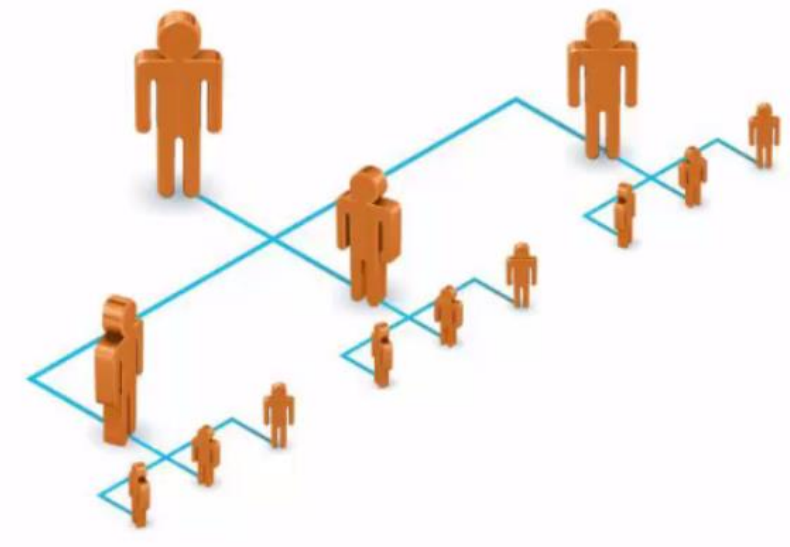
- Intercloud Interoperability and Federation
- Requirements
- Advantages
- Participants

Intercloud Interoperability



Management Recommendations

- Data Migration
  - Continuity of Operations
  - Compliance
  - Administrator staff
- Legal
  - Operating process
  - Acceptable use policies
  - Licensing
  - Patch Management



Data Governance Recommendations

- Data Access Standards
- Data Separation
- Data Integrity
- Data Regulations
- Data Disposition
- Data Recovery

Security and Reliability Recommendations

- Consumer side vulnerabilities
- Encryption
- Physical
- Authentication
- Identity and access management
- Performance Requirements

Virtual Machine Recommendations

- VM Vulnerabilities
  - Other VMs
  - Host
  - Network
- VM Migration

Software and Application Recommendations

- Time Critical Software
- Safety Critical Software
- Application Development Tools
- Application Run time support
- Application configuration
- Standard programming languages

Success Factors

- Trust
- Core Competency
- Relational, Technical and managerial capabilities

Tutorial - Summary

- Critical
- Rigorous Decision Making process
- Comply with standards
- Compare all alternatives
- Use Best Practices