

Chapter 22

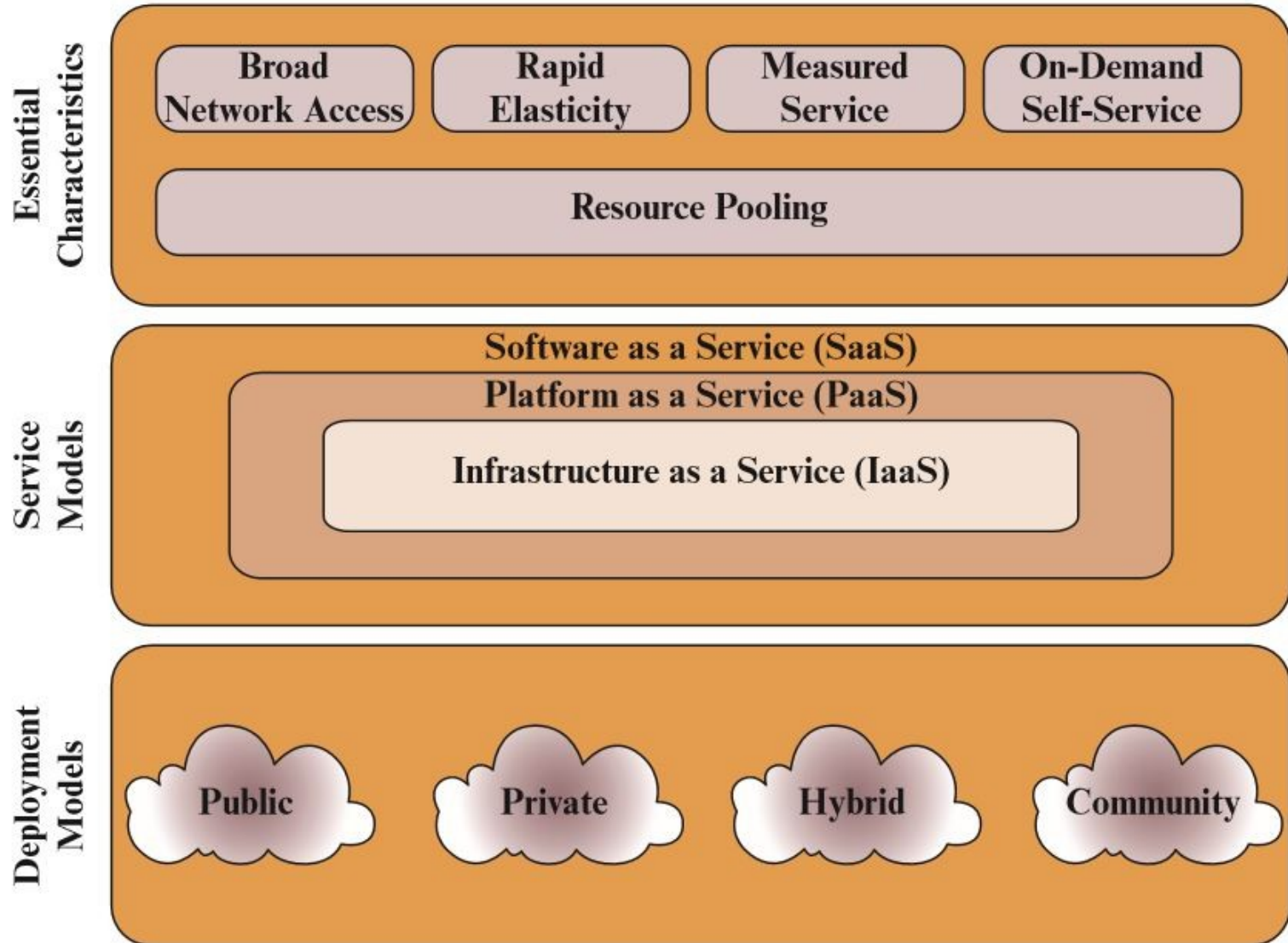
Cloud Security

Cloud Computing

- NIST defines cloud computing, in NIST SP-800-145 (*The NIST Definition of Cloud Computing*), as follows:

Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models

Cloud Computing Elements



Cloud Service Models

NIST defines three service models, which can be viewed as nested service alternatives:

Software as a
service
(SaaS)

Platform as a
service
(PaaS)

Infrastructure
as a service
(IaaS)

Software as a Service (SaaS)

- SaaS provides service to customers in the form of software, specifically application software, running on and accessible in the cloud
- SaaS enables the customer to use the cloud provider's applications running on the provider's cloud infrastructure
- The applications are accessible from various client devices through a simple interface such as a Web browser
- Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service
- The use of SaaS avoids the complexity of software installation, maintenance, upgrades, and patches

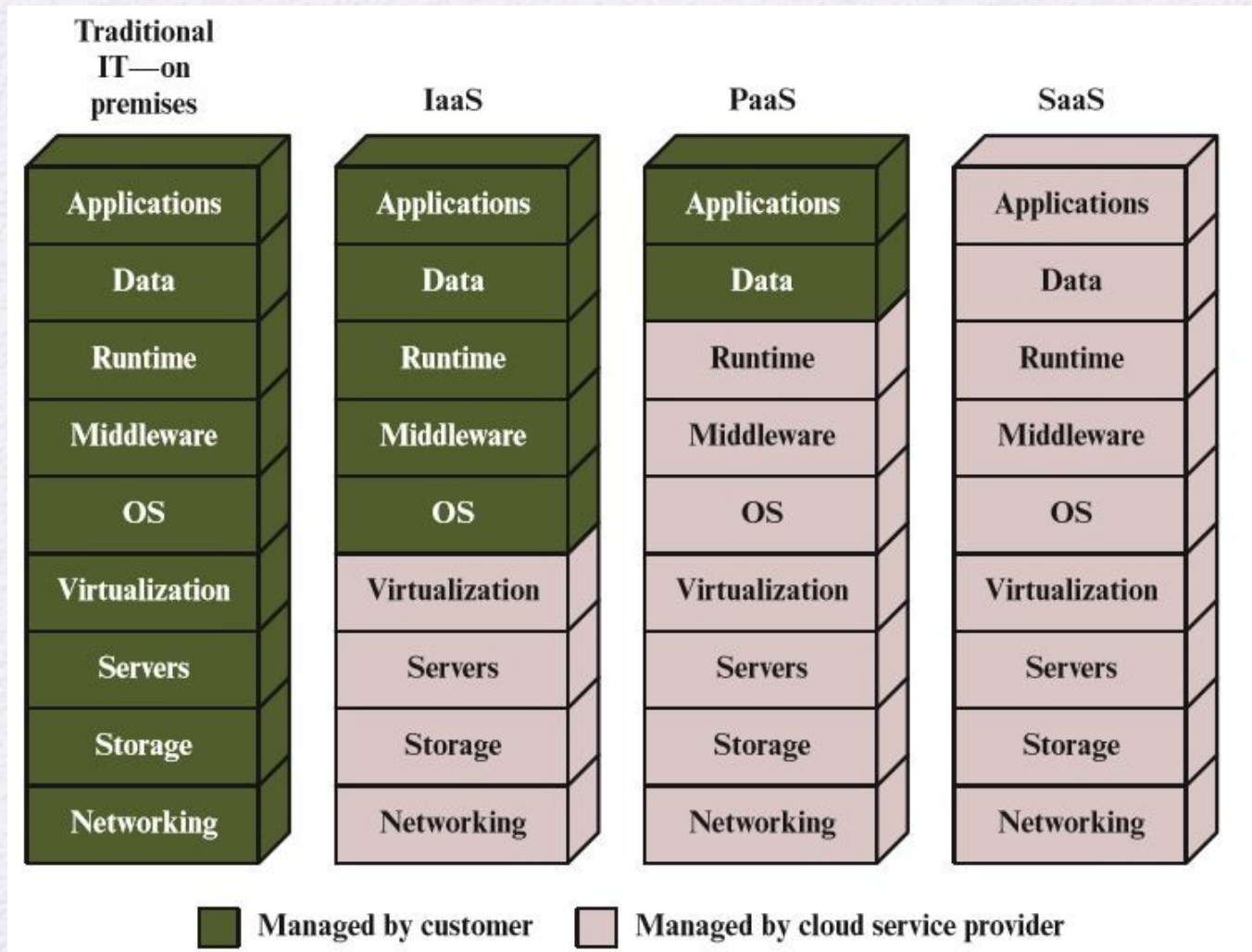
Platform as a Service (PaaS)

- A PaaS cloud provides service to customers in the form of a platform on which the customer's applications can run
- PaaS enables the customer to deploy onto the cloud infrastructure customer-created or acquired applications
- A PaaS cloud provides useful software building blocks, plus a number of development tools, such as programming language tools, run-time environments, and other tools that assist in deploying new applications
- In effect, PaaS is an operating system in the cloud
- PaaS is useful for an organization that wants to develop new or tailored applications while paying for the needed computing resources only as needed and only for as long as needed

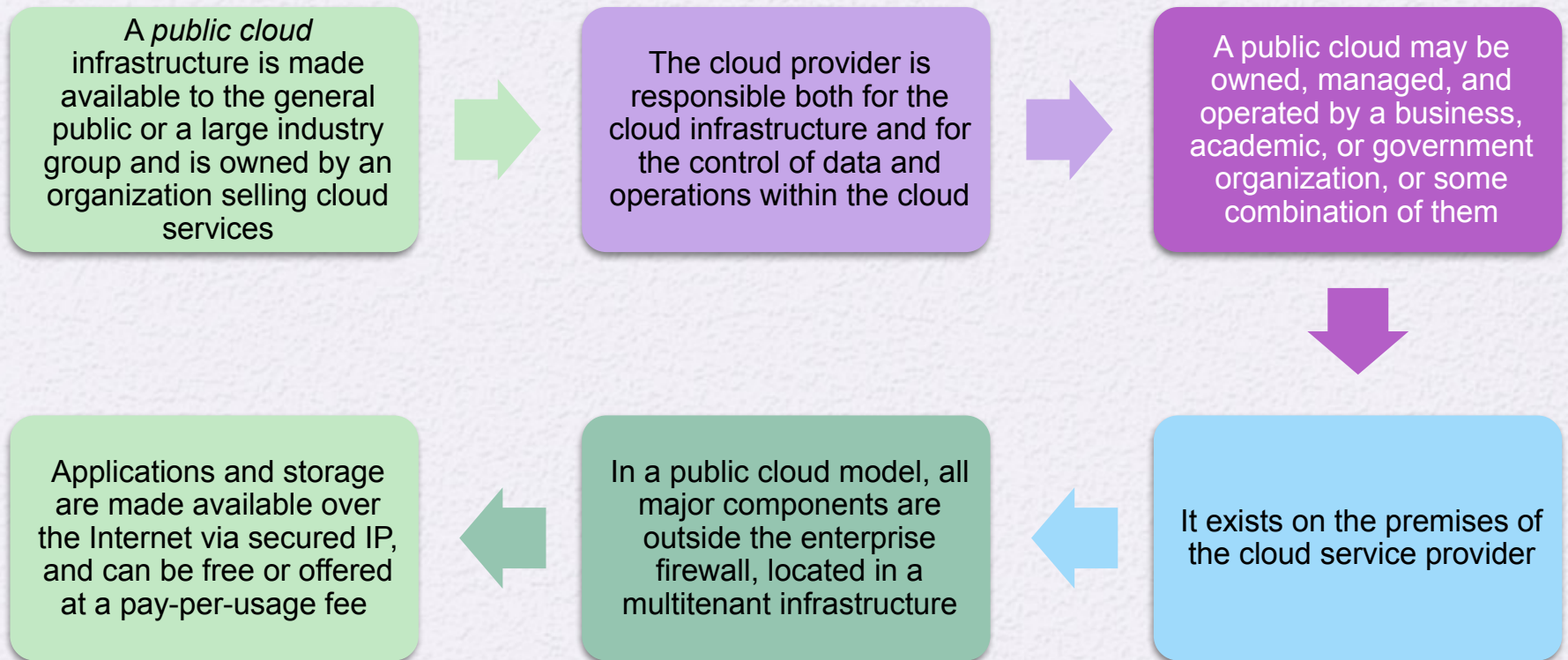
Infrastructure as a Service (IaaS)

- With IaaS, the customer has access to the resources of the underlying cloud infrastructure
- The cloud service user does not manage or control the resources of the underlying cloud infrastructure but has control over operating systems, deployed applications, and possibly limited control of select networking components
- IaaS provides virtual machines (VMs) and other virtualized hardware and operating systems
- IaaS offers the customer processing, storage, networks, and other fundamental computing resources so that the customer is able to deploy and run arbitrary software, which can include operating systems and applications
- IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems
- Typically, customers are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment
- API access to the infrastructure may also be offered as an option

Separation of Responsibilities in Cloud Service Models



Public Cloud



Public Cloud

While public clouds are inexpensive and scale to meet needs, they typically provide no or lower service level agreements (SLAs) and may not offer the guarantees against data loss or corruption found with private or hybrid cloud offerings



The public IaaS clouds do not necessarily provide for restrictions and compliance with privacy laws, which remain the responsibility of the subscriber or corporate end user

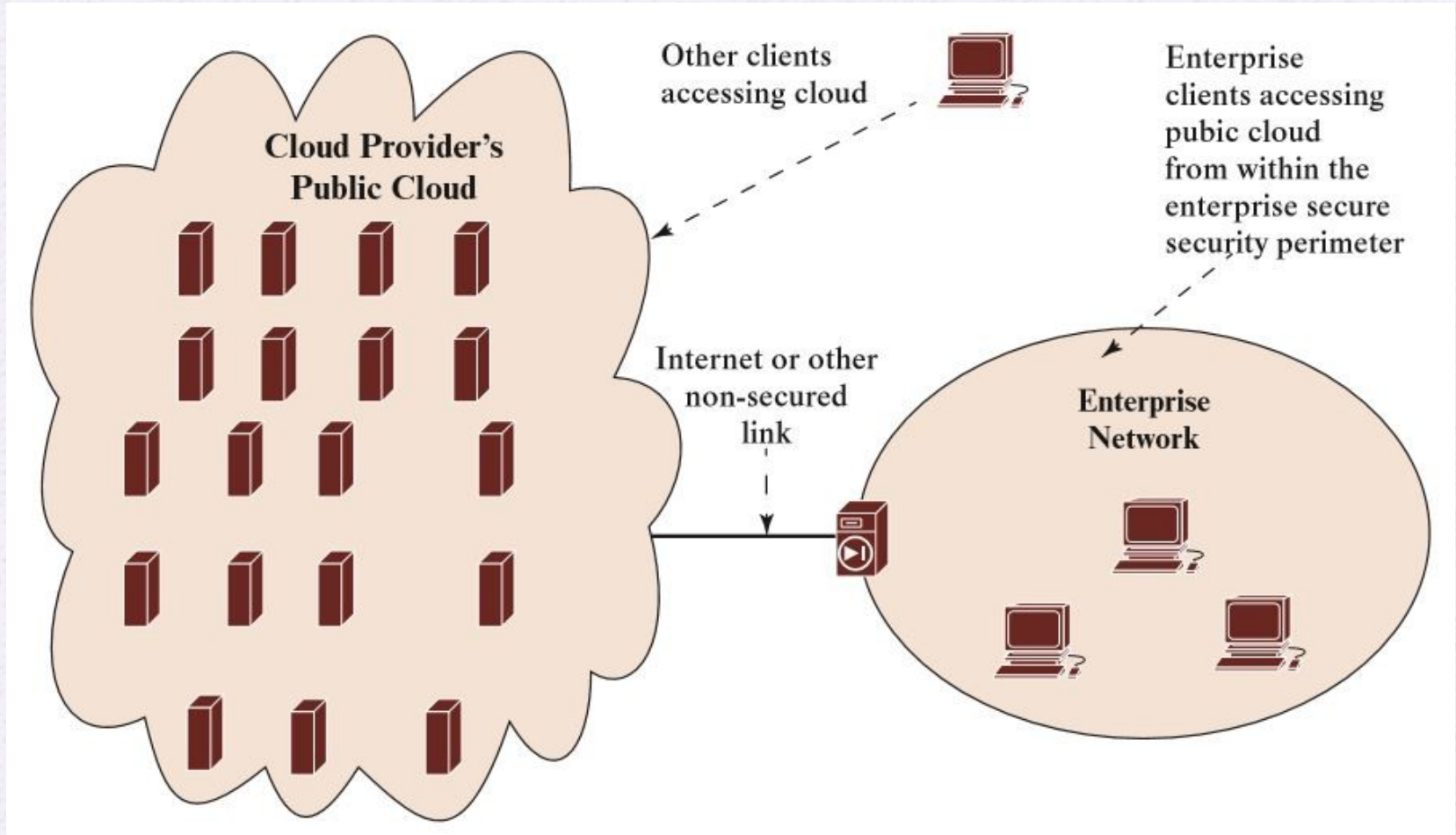


The principal concern is security



The major advantage of the public cloud is cost

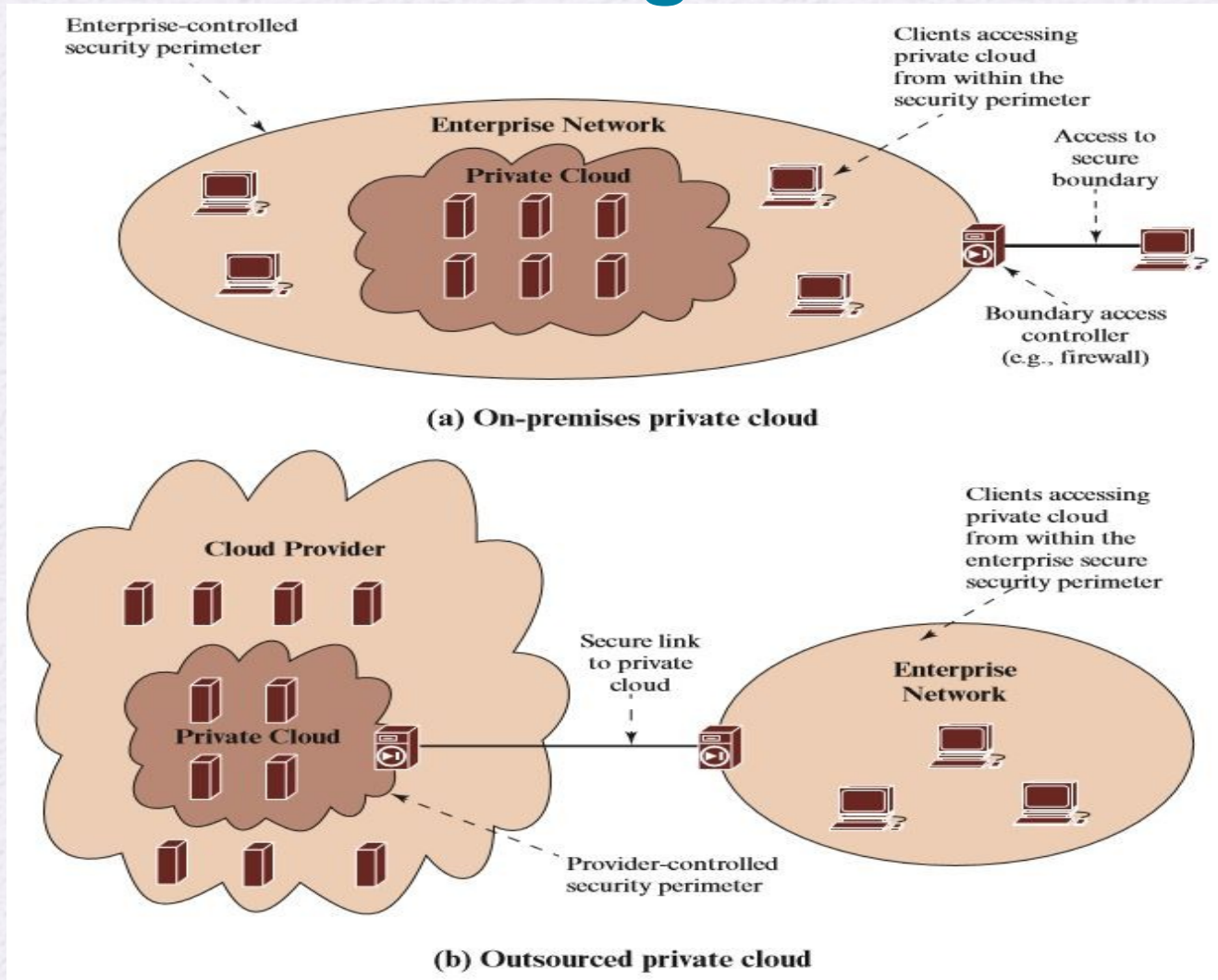
Public Cloud Configuration



Private Cloud

- A *private cloud* is implemented within the internal IT environment of the organization
- The organization may choose to manage the cloud in house or contract the management function to a third party
- Additionally, the cloud servers and storage devices may exist on premise or off premise
- Private clouds can deliver IaaS internally to employees or business units through an intranet or the Internet via a virtual private network (VPN), as well as software (applications) or storage as services to its branch offices
- A key motivation for opting for a private cloud is security
- Other benefits include easy resource sharing and rapid deployment to organizational entities

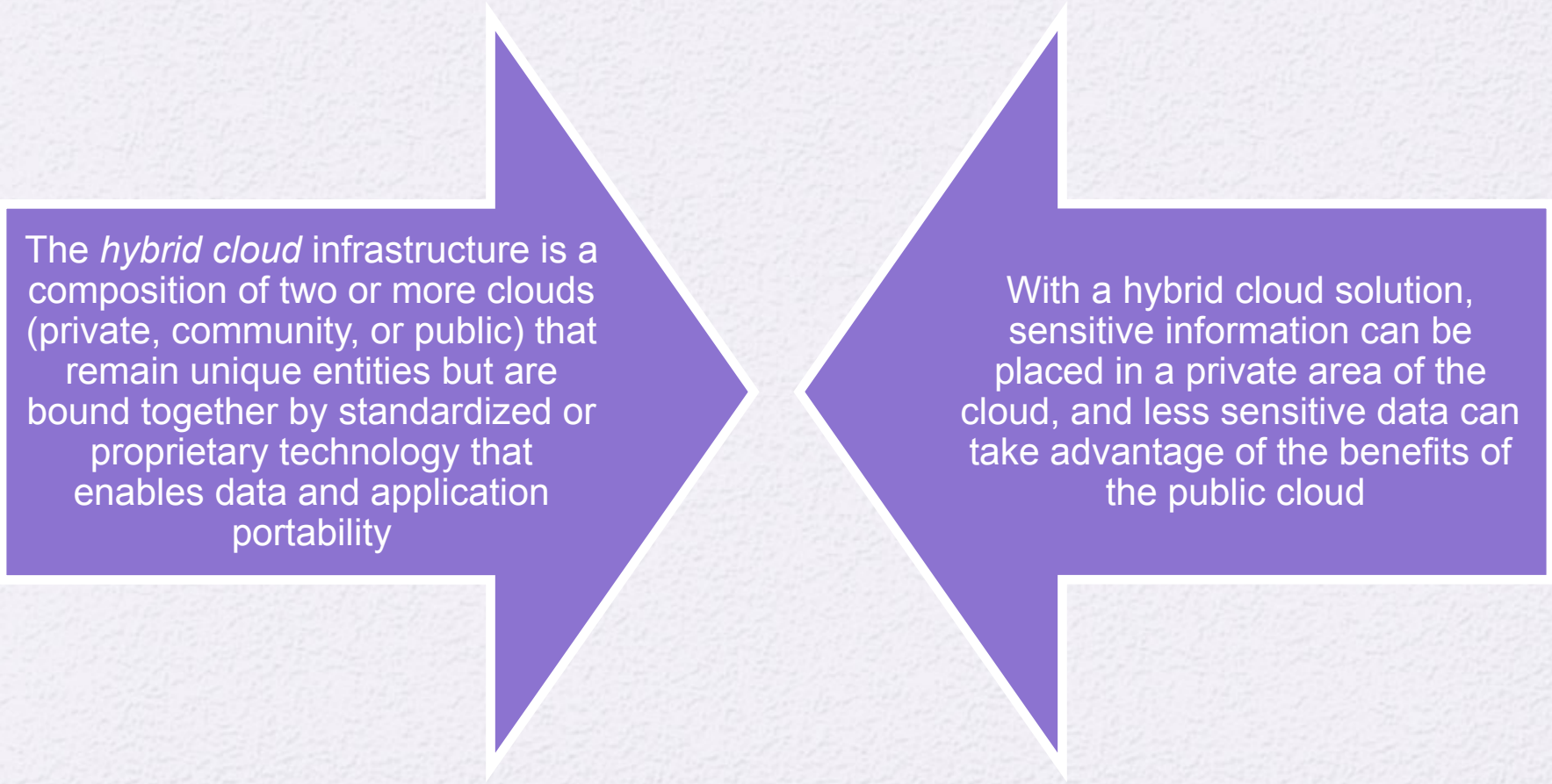
Private Cloud Configurations



Community Cloud

- A *community cloud* shares characteristics of private and public clouds
- Like a private cloud, a community cloud has restricted access
- Like a public cloud, the cloud resources are shared among a number of independent organizations
- The organizations that share the community cloud have similar requirements and, typically, a need to exchange data with each other
- A community cloud can be implemented to comply with government privacy and other regulations
- The cloud infrastructure may be managed by the participating organizations or a third party and may exist on premise or off premise

Hybrid Cloud



The *hybrid cloud* infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

With a hybrid cloud solution, sensitive information can be placed in a private area of the cloud, and less sensitive data can take advantage of the benefits of the public cloud

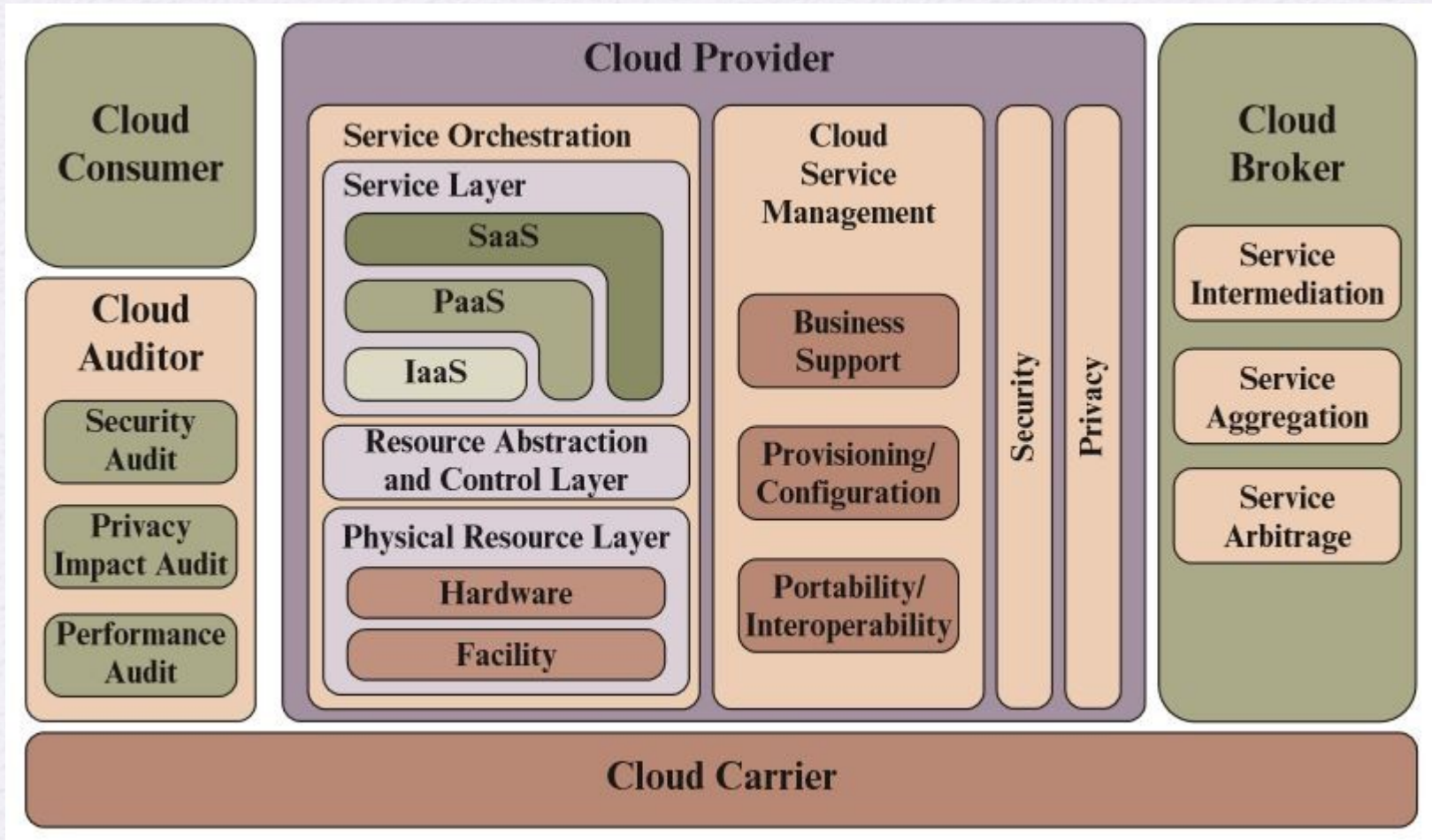
Comparison of Cloud Deployment Models

	Private	Community	Public	Hybrid
Scalability	Limited	Limited	Very high	Very high
Security	Most secure option	Very secure	Moderately secure	Very secure
Performance	Very good	Very good	Low to medium	Good
Reliability	Very high	Very high	Medium	Medium to high
Cost	High	Medium	Low	Medium

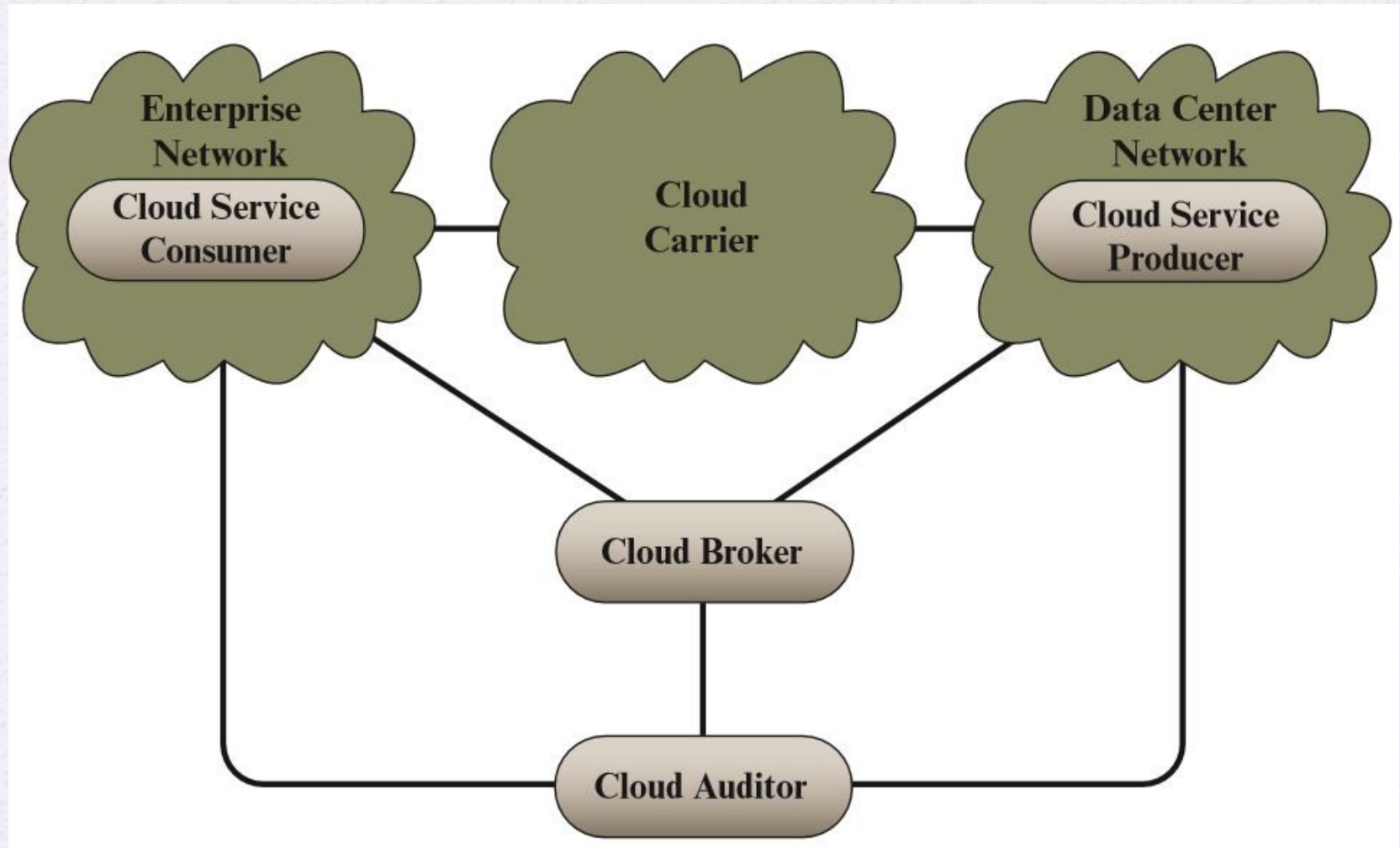
Cloud Computing Reference Architecture

- A cloud computing reference architecture depicts a generic high-level conceptual model for discussing the requirements, structures, and operations of cloud computing
- NIST SP 500-292 (*NIST Cloud Computing Reference Architecture*) establishes a reference architecture, described as follows:
 - The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation
 - The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing

NIST Cloud Computing Reference Architecture



Interactions Between Actors in Cloud Computing



NIST Guidelines on Security and Privacy Issues and Recommendations

Page 1 of 2

Governance

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.

Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Trust

Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.

Establish clear, exclusive ownership rights over data.

Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.

Continuously monitor the security state of the information system to support ongoing risk management decisions.

Architecture

Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

Identity and access management

Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software isolation

Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

NIST Guidelines on Security and Privacy Issues and Recommendations

Page 2 of 2

Data protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

Take into consideration the risk of collating organizational data with those of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

Availability

Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.

Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.

Incident response

Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.

Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.

Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

The Cloud Security Alliance lists 12 top cloud-specific security threats, in decreasing order of severity:

- 1. Data Breaches**
- 2. Weak Identity, Credential and Access Management**
- 3. Insecure APIs**
- 4. System and Application Vulnerabilities**
- 5. Account Hijacking**
- 6. Malicious Insiders**
- 7. Advanced Persistent Threats (APTs)**
- 8. Data Loss**
- 9. Insufficient Due Diligence**
- 10. Abuse and Nefarious Use of Cloud Services**
- 11. Denial-of-Service**
- 12. Shared Technology Vulnerabilities**

Revised 2019

Top Threats to Cloud Computing

The Egregious 11

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

Source: Cloud Security Alliance



The Egregious 11 - analysis

There is a drop in the ranking of traditional cloud security issues under the responsibility of cloud service providers (CSPs). Concerns such as denial of service, shared technology vulnerabilities and CSP data loss and system vulnerabilities—which all featured in the previous Treacherous 12—were now rated so low they have been excluded in this report.

These omissions suggest that traditional security issues under the responsibility of the CSP seem to be less of a concern. Instead, we're seeing more of a need to address security issues that are situated higher up the technology stack that are the result of senior management decisions.

New, highly rated items in the survey are more nuanced and suggest a maturation of the consumer's understanding of the cloud. These issues are inherently specific to the cloud and thus indicate a technology landscape where consumers are actively considering cloud migration. Such topics refer to potential control plane weaknesses, metastructure and applistructure failures and limited cloud visibility. This new emphasis is markedly different from more generic threats, risks and vulnerabilities (i.e. data loss, denial of service) that featured more strongly in previous Top Threats reports.

STRIDE Threat Model

- STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions
- **Spoofing identity:** An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password
 - Security controls to counter such threats are in the area of **authentication**
- **Tampering with data:** Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
 - Relevant security controls are in the area of **integrity**

STRIDE Threat Model

- **Repudiation:** Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise
 - Relevant security controls are in the area of **non-repudiation**, which refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
- **Information disclosure:** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
 - Relevant security controls are in the area of **confidentiality**

STRIDE Threat Model

- **Denial-of-Service:** Denial-of-Service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable
 - Relevant security controls are in the area of **availability**
- **Elevation of privilege:** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself
 - Relevant security controls are in the area of **authorization**

Mapping Between Cloud Threats and the STRID E Model

	S	T	R	I	D	E
Data Breaches				✓		
Weak Identity, Credential and Access Management	✓	✓	✓	✓	✓	✓
Insecure APIs		✓	✓	✓		✓
System Vulnerabilities	✓	✓	✓	✓	✓	✓
Account Hijacking	✓	✓	✓	✓	✓	✓
Malicious Insiders	✓	✓		✓		
Advanced Persistent Threats (APTs)				✓		✓
Data Loss			✓		✓	
Insufficient Due Diligence	✓	✓	✓	✓	✓	✓
Abuse and Nefarious Use of Cloud Services					✓	
Denial of Service					✓	
Shared Technology Vulnerabilities				✓		✓

S = Spoofing identity; I = Information disclosure

T = Tampering with data; D = Denial-of-service

R = Repudiation; E = Elevation of privilege.

(Table is on page 695 in the textbook)

Data Breaches

- A data breach is an incident in which sensitive, protected, or confidential information is released, viewed, stolen, or used by an individual who is not authorized
- The threat of data compromise increases in the cloud
 - This is due to the number of, and interactions between, risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment

Data Breaches

- Database environments used in cloud computing can vary significantly
 - Multi-instance model
 - Provides a unique DBMS running on a VM instance for each cloud subscriber
 - This gives the subscriber complete control over role definition, user authorization, and other administrative tasks related to security
 - Multitenant model
 - Provides a predefined environment for the cloud subscriber that is shared with other tenants typically through tagging data with a subscriber identifier
 - Tagging gives the appearance of exclusive use of the instance, but relies on the cloud provider to establish and maintain a sound secure database environment

Data Breaches

- Data must be secured while at rest, in transit, and in use, and access to the data must be controlled
 - The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CSP
 - The client can enforce access control techniques but the CSP is involved to some extent depending on the service model used
 - For data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CSP having no access to the encryption key
 - So long as the key remains secure, the CSP has no ability to decipher the data, although corruption and other DoS attacks remain a risk

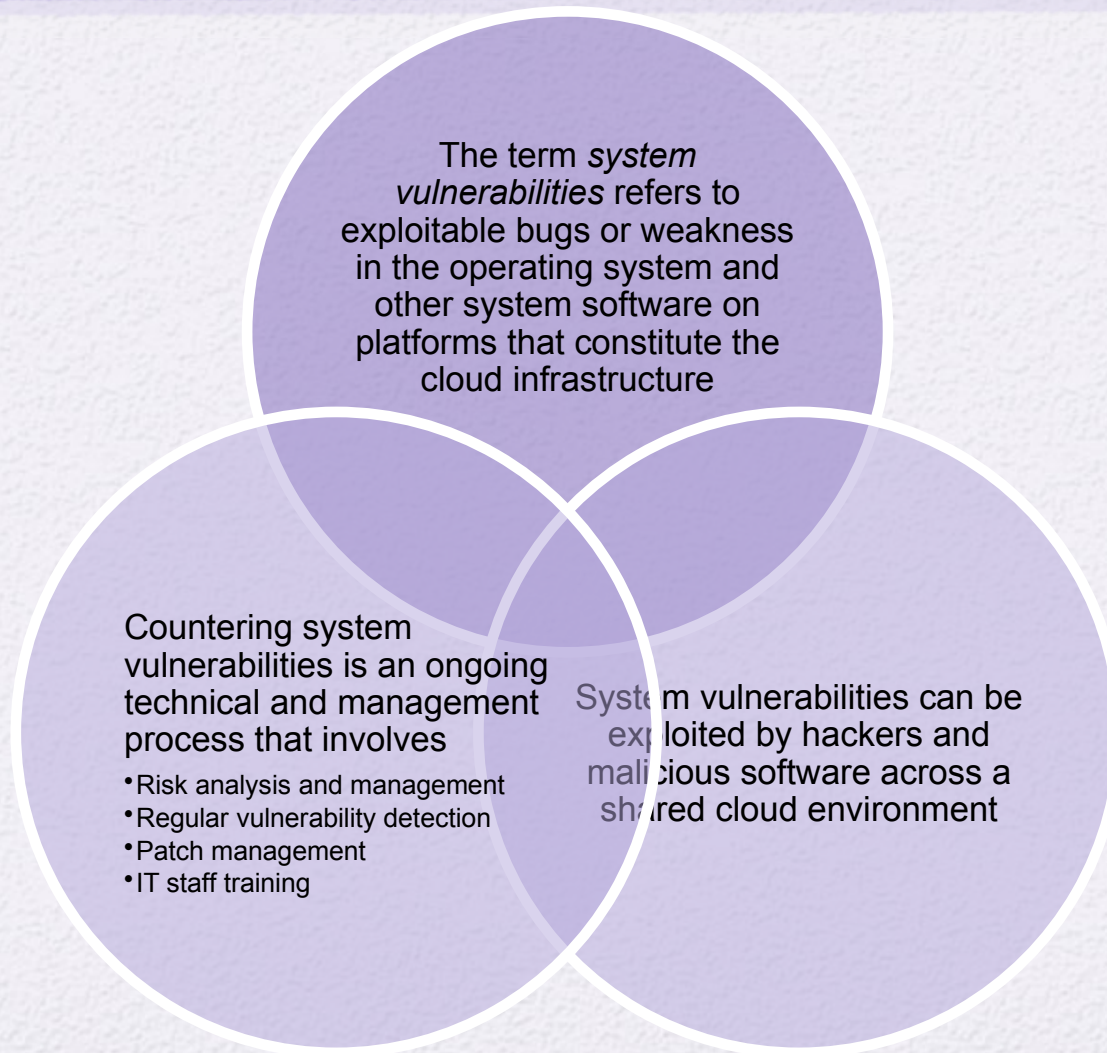
Identity and Access Management (IAM)

- Includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, and then granting the correct level of access based on this assured identity
 - Identity provisioning
 - Providing access to identified users and subsequently denying access to users when the client enterprise designates such users as no longer having access to enterprise resources in the cloud
 - Another aspect of identity management is for the cloud to participate in the identity management scheme used by the client enterprise
 - The cloud service provider must be able to exchange identity attributes with the enterprise's chosen identity provider
 - The access management portion of IAM involves authentication and access control services
 - The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way

Insecure APIs

- CSPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services
- The security and availability of general cloud services are dependent upon the security of these basic APIs
- From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy
- Countermeasures include:
 - (1) Analyzing the security model of CSP interfaces
 - (2) Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission
 - (3) Understanding the dependency chain associated with the API

System Vulnerabilities



Account Hijacking

- Account or service hijacking remains a top threat
- With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services
- The concern is heightened in the context of cloud computing because:
 - There is additional attack surface exposure due to increased complexity and dynamic infrastructure allocation
 - New APIs/interfaces are emerging that are untested
 - The consumer's account, if hijacked, may be used to steal information, manipulate data, and defraud others, or to attack other tenants as an insider in the multi-tenancy environment
- Countermeasures include the following
 - (1) Prohibit the sharing of account credentials between users and services
 - (2) Leverage strong two-factor authentication techniques where possible
 - (3) Employ proactive monitoring to detect unauthorized activity
 - (4) Understand CSP security policies and SLAs

Malicious Insiders

- Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the CSP
 - One grave concern is the risk of malicious insider activity
 - Cloud architectures necessitate certain roles that are extremely high risk
 - Examples include CSP system administrators and managed security service providers
- Countermeasures include the following:
 - 1) Enforce strict supply chain management and conduct a comprehensive supplier assessment
 - 2) Specify human resource requirements as part of legal contract
 - 3) Require transparency into overall information security and management practices, as well as compliance reporting
 - 4) Determine security breach notification processes

Advanced Persistent Threats (APT)

A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time

The intention of an APT attack is to steal data rather than to cause damage to the network or organization

APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry

APTs differ from other types of attack by their careful target selection, and persistent, often stealthy, intrusion efforts over extended periods

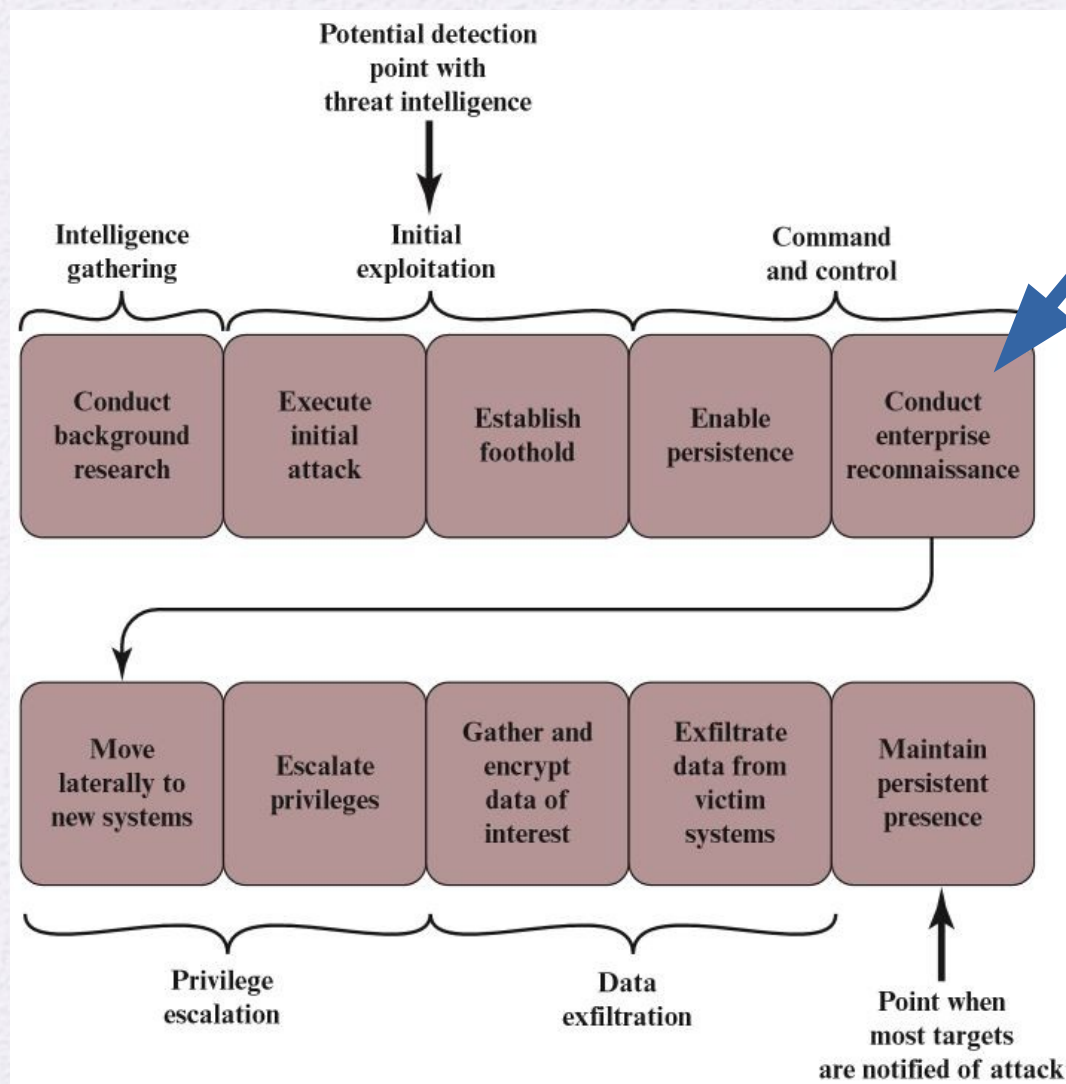
Advanced Persistent Threats (APT)

The principle countermeasure for such threats is the effective use of threat intelligence

Threat intelligence is helping organizations understand the risks of the most common and severe external threats, such as advanced persistent threats (APTs), exploits, and zero-day threats

Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage

Threat Intelligence for Countering Advanced Persistent Threats



Living Off the Land Attacks (LOTL)

Data Loss

Data loss refers to the permanent loss of CSC data that are stored in the cloud through accidental or malicious deletion of data and backup copies from cloud storage

To counter this threat, the CSC should be assured that the CSP has a thorough redundancy scheme with regular backups, including geographic redundancy

This may be supplemented by a cloud-to-premise backup so that a recent copy is available at the customer site

Categories of Due Diligence

Verify infrastructure

- The CSPs infrastructure consists of facilities, hardware, system and application software, core connectivity, and external network interfaces
- The CSP should rely on standardized, enterprise class equipment, and software with documented integration schemes

Verify certification

- At minimum, the CSP should demonstrate that it is in compliance with all relevant security and privacy laws and regulations
- In addition, the CSP should follow industry best practices as documented in numerous NIST documents, specifications from the Cloud Security Alliance, and various industry and standards organization specifications

Verify the CSP's due diligence

- The CSP must document and, as appropriate, demonstrate that it is doing its own due diligence to ensure that its equipment, networks, and protocols actually work through a broad spectrum of scenarios, both ordinary and catastrophic

Verify data protection

- The CSP should be able to document a comprehensive and integrated set of security controls to ensure against data breaches and data loss

Abuse and Nefarious Use of Cloud Services

- For many CSPs, it is relatively easy for a CSC to register and begin using cloud services, some even offering free limited trial periods; this enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and DoS
- PaaS providers have traditionally suffered most from this kind of attack; however, recent evidence shows that hackers have begun to target IaaS vendors as well
- The burden is on the CSP to protect against such attacks, but CSCs must monitor activity with respect to their data and resources to detect any malicious behavior
- Countermeasures include:
 - (1) Stricter initial registration and validation processes
 - (2) Enhanced credit card fraud monitoring and coordination
 - (3) Comprehensive introspection of customer network traffic
 - (4) Monitoring public blacklists for one's own network blocks

Denial-of-Service

- By the nature of the service it provides, a public CSP has to be exposed to the Internet and other public networks, its presence advertised, and its interfaces well-defined
- These factors make CSPs a logical target for DoS attacks
- Such attacks can prevent, for a time, a CSC from accessing their data or their applications
- The countermeasure for such attacks is for the CSP
 - (1) To perform ongoing threat intelligence to be aware of the nature of potential attacks and the potential vulnerabilities in their cloud
 - (2) To deploy automated tools to spot and defend the core cloud services from such attacks

Shared Technology Vulnerabilities

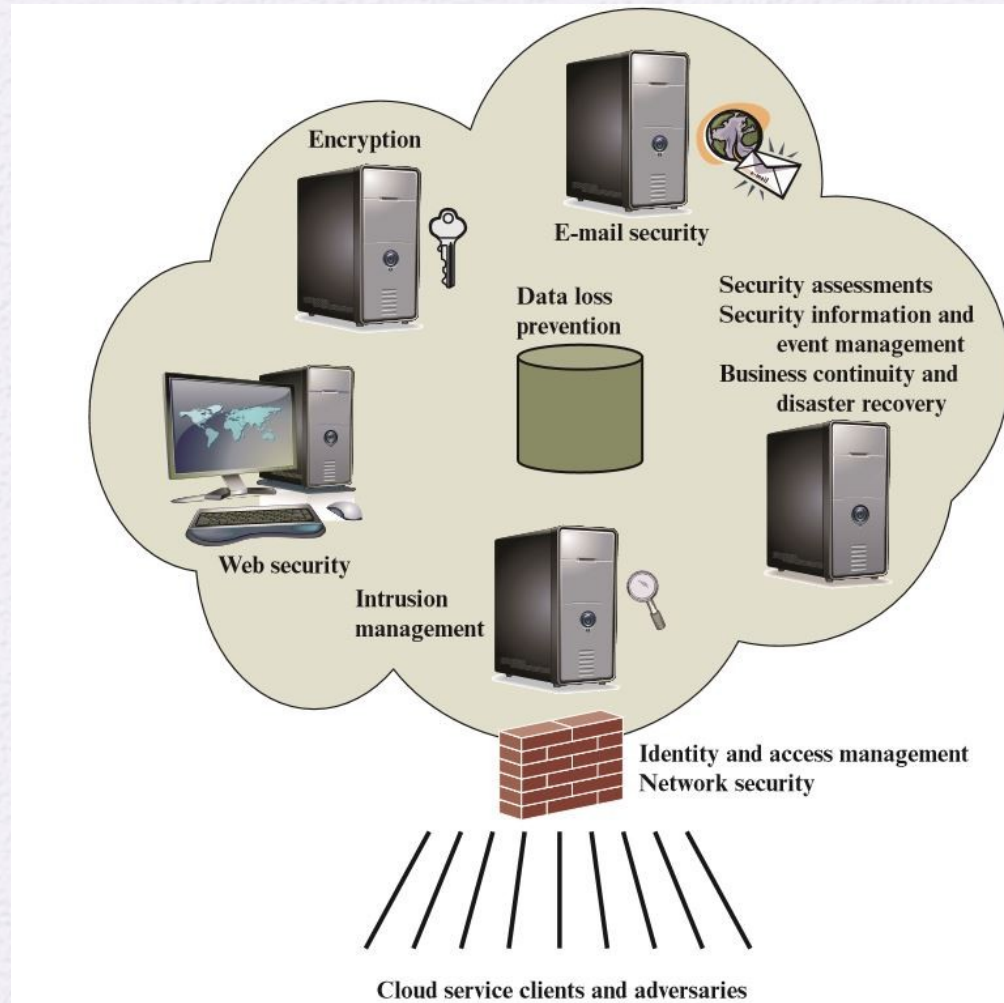
- IaaS vendors deliver their services in a scalable way by sharing infrastructure
 - Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture
- Countermeasures include the following:
 - (1) Implement security best practices for installation/configuration
 - (2) Monitor environment for unauthorized changes/ activity
 - (3) Promote strong authentication and access control for administrative access and operations
 - (4) Enforce SLAs for patching and vulnerability remediation
 - (5) Conduct vulnerability scanning and configuration audits

Cloud Security as a Service (SecaaS)

- ★ The Cloud Security Alliance defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems
- ★ The Cloud Security Alliance has identified the following SecaaS categories of service:
 - ★ Identity and access management
 - ★ Data loss prevention
 - ★ Web security
 - ★ E-mail security
 - ★ Security assessments
 - ★ Intrusion management
 - ★ Security information and event management
 - ★ Encryption
 - ★ Business continuity and disaster recovery
 - ★ Network security



Elements of Cloud Security as a Service



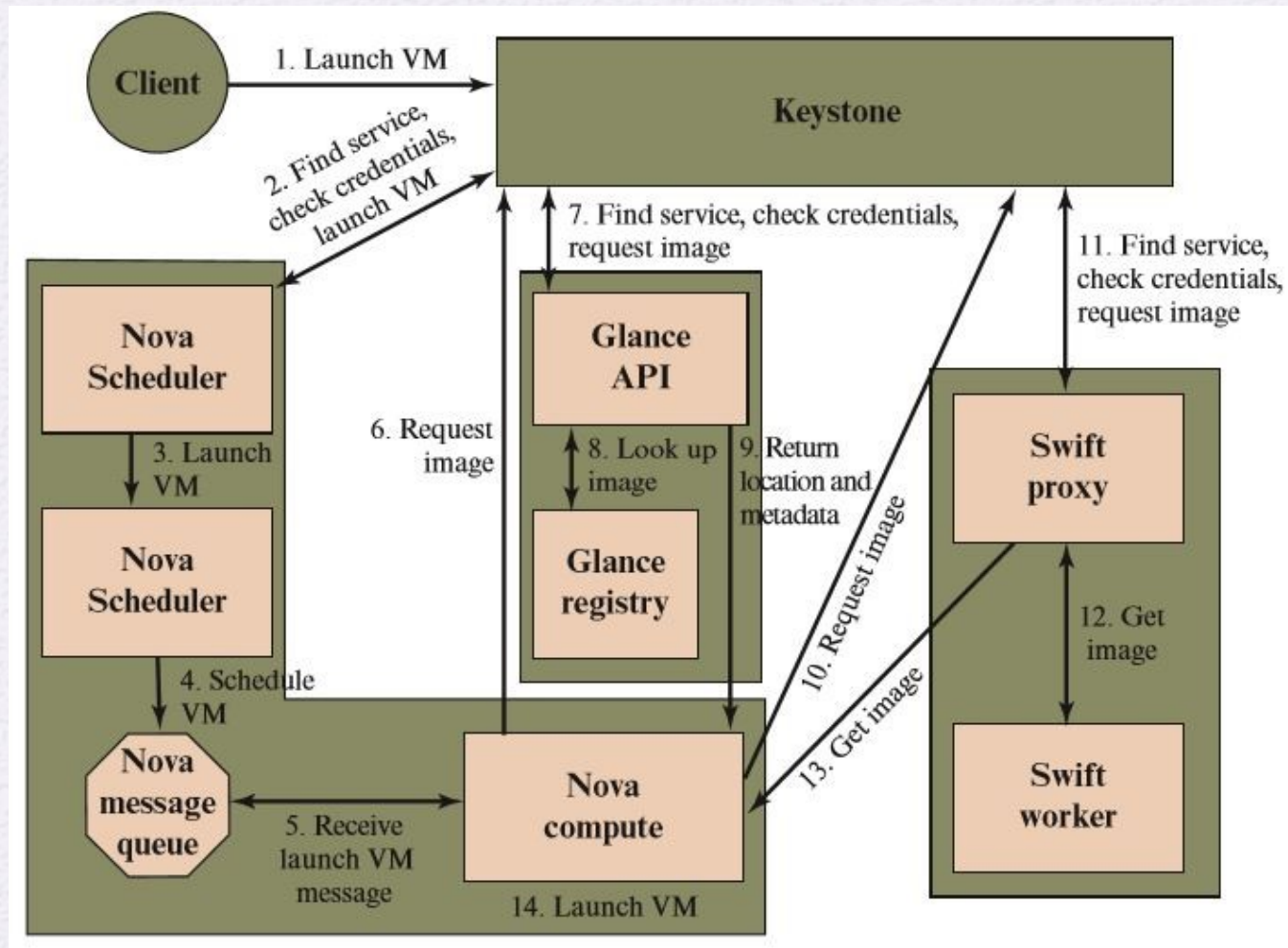
OpenStack

- OpenStack is an open source software project of the OpenStack Foundation that aims to produce an open source cloud operating system
- The principal objective is the enable creating and managing huge groups of virtual private servers in a cloud computing environment
- OpenStack is embedded, to one degree or another, into data center infrastructure and cloud computing products offered by Cisco, IBM, Hewlett-Packard, and other vendors
- It provides multi-tenant IaaS, and aims to meet the needs of public and private clouds regardless of size
- The OpenStack OS consists of a number of independent modules, each of which has a project name and a functional name
- Typically the components are configured together to provide a comprehensive IaaS capability
- The modular design is such that the components are generally capable of being used independently

OpenStack

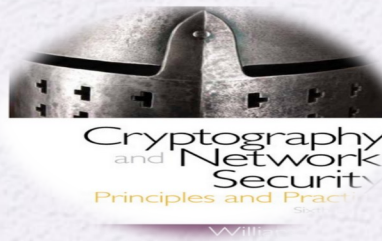
- The security module for OpenStack is Keystone
- Keystone provides the shared security services essential for a functioning cloud computing infrastructure
- It provides the following main services:
 - Identity
 - Token
 - Service catalog
 - Policies

Launching a Virtual Machine in OpenStack



Summary

- Present an overview of cloud computing concepts
- List and define the principal cloud services
- List and define the cloud deployment models
- Explain the NIST cloud computing reference architecture



- Understand the unique security issues related to cloud computing
- Describe Cloud Security as a Service
- Understand the OpenStack security module for cloud security