HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN MẠNG NÂNG CAO

CHƯƠNG 4 – BẢO MẬT CHO ĐIỆN TOÁN ĐÁM MÂY

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

NỘI DUNG CHƯƠNG 4

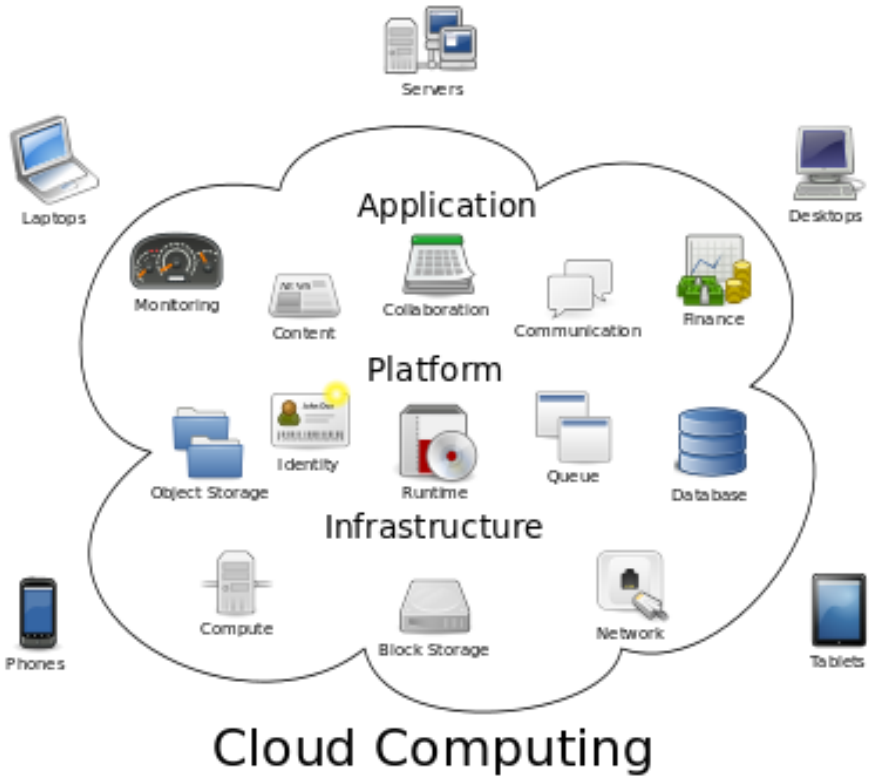
1. Điện toán đám mây là gì (ĐTĐM)?
2. Kiến trúc của điện toán đám mây
3. Lợi ích của điện toán đám mây
4. Các công nghệ nền tảng xây dựng ĐTĐM
5. Tính toán lưới và ĐTĐM
6. Một số nhà cung cấp dịch vụ và ứng dụng của ĐTĐM
7. Vấn đề bảo mật trong ĐTĐM

4.1 Điện toán đám mây là gì?

❖ Điện toán đám mây (Cloud Computing) là gì?

Điện toán đám mây là gì (tiếp)?

- Điện toán đám mây (Cloud Computing) là gì?
  - Theo Wikipedia.org:
    - Cloud computing, also known as *on-demand computing*, is a kind of *internet-based computing*, where shared resources and information are provided to computers and other devices on-demand.
    - It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources.

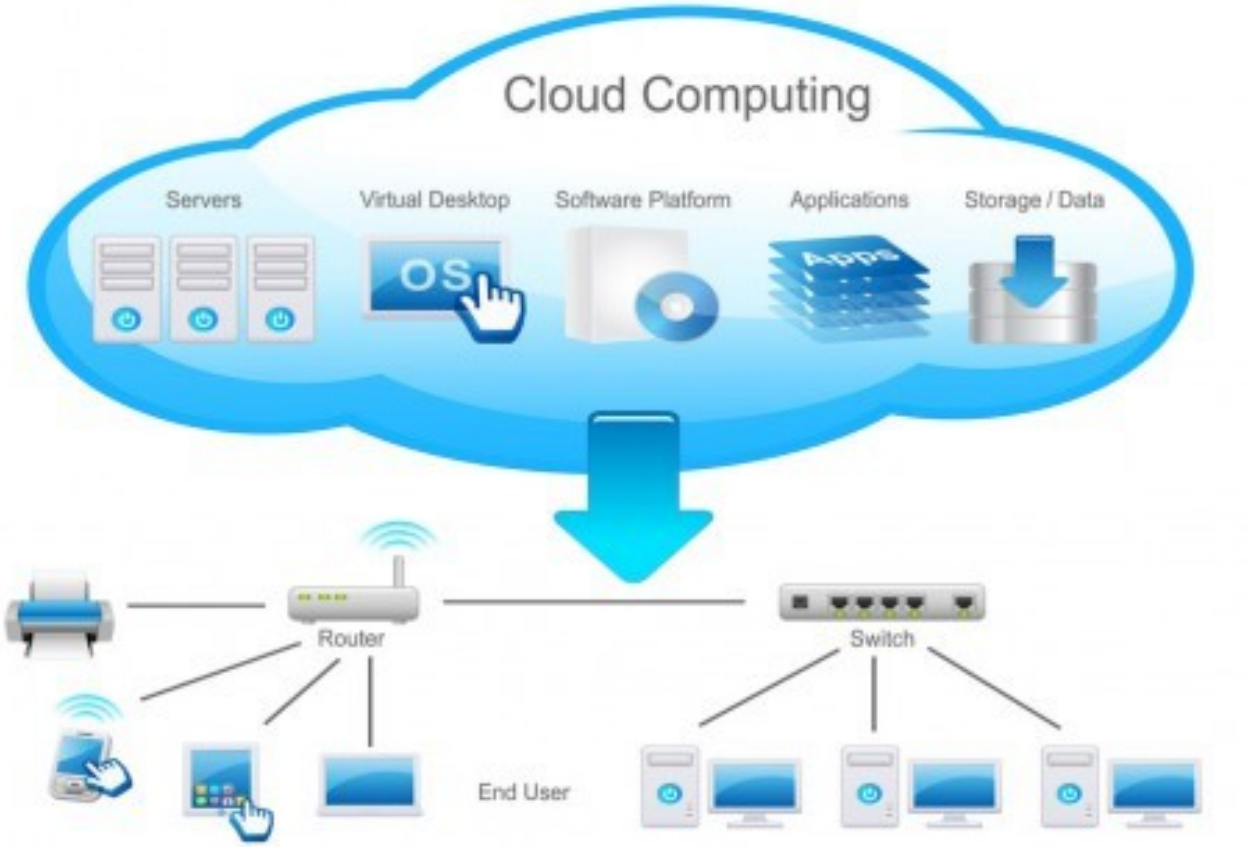


Điện toán đám mây là gì (tiếp)?

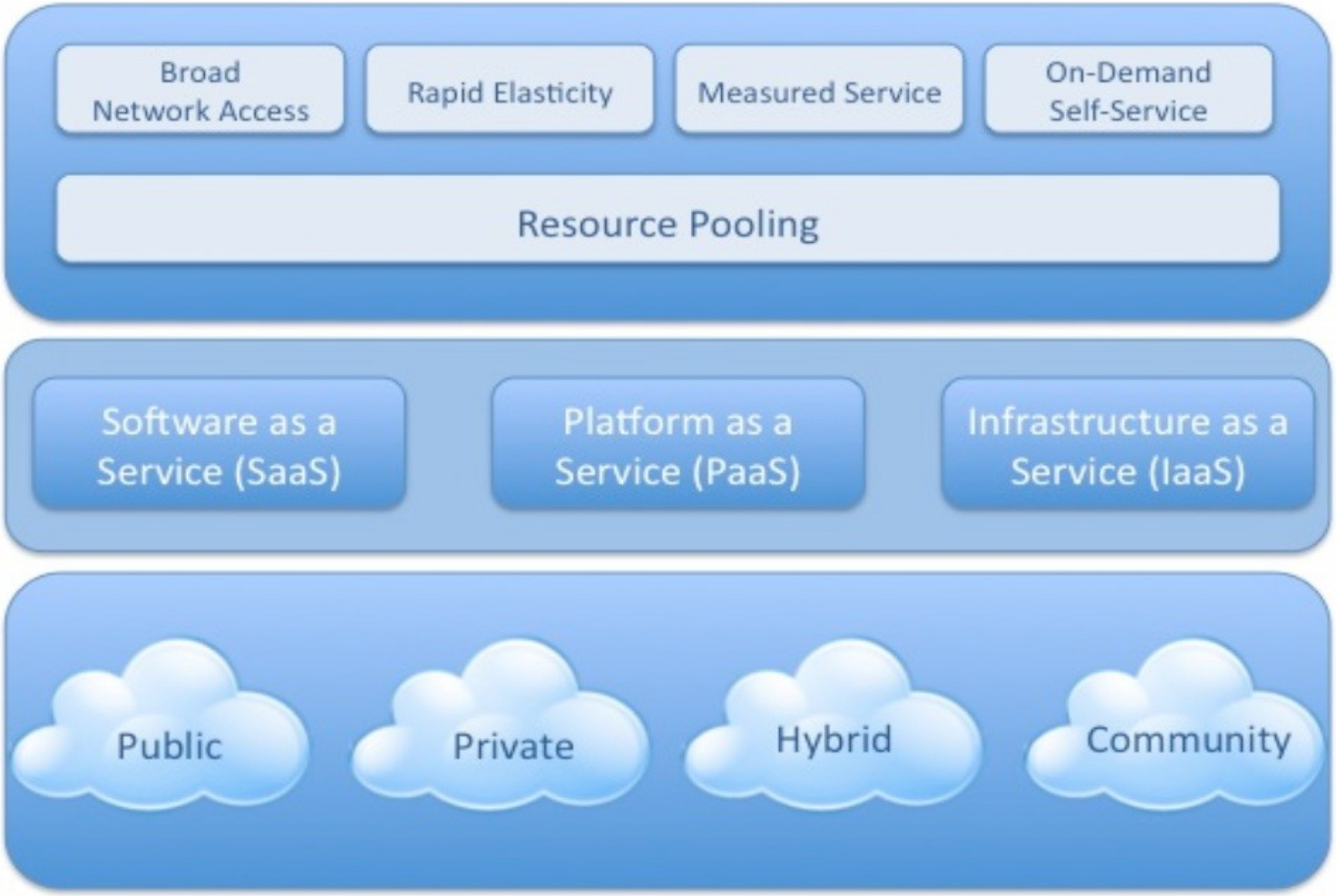
- Điện toán đám mây (Cloud Computing) là gì?
  - Theo Webopedia.com:
    - Cloud computing is defined as a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications.
    - In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "*a type of Internet-based computing*," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.

Điện toán đám mây là gì (tiếp)?

- Điện toán đám mây (Cloud Computing) là gì?
  - Theo Webopedia.com:



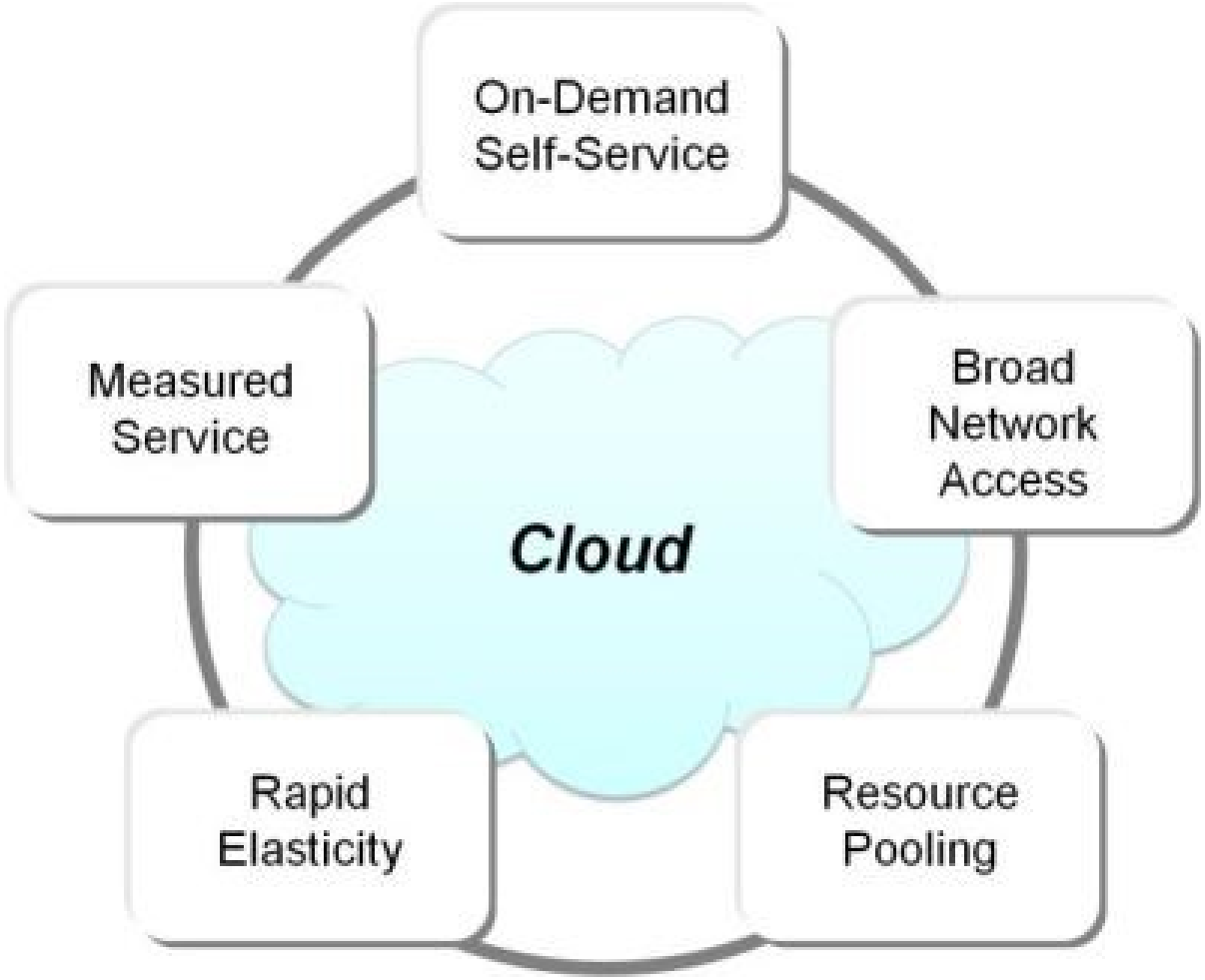
4.2 Kiến trúc của điện toán đám mây



Kiến trúc của điện toán đám mây (tiếp)

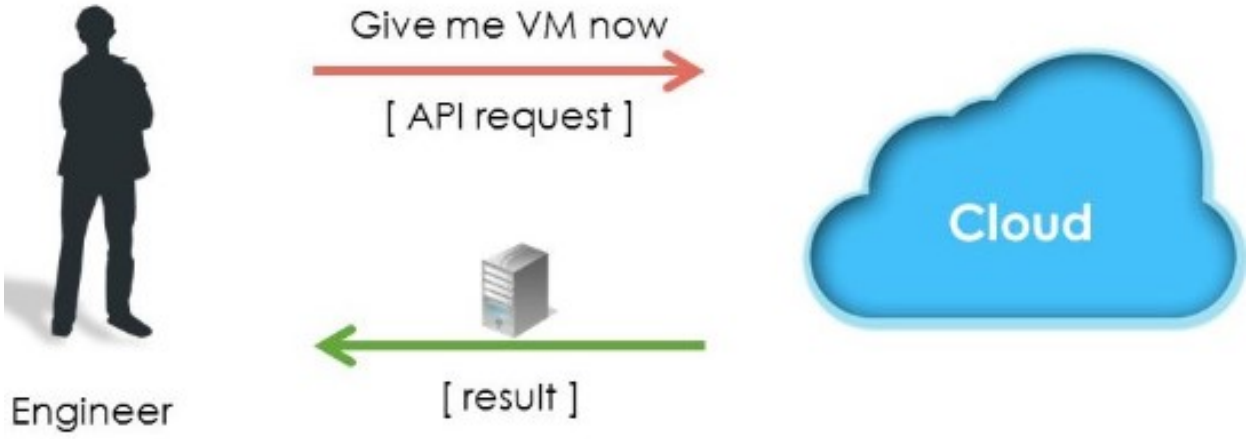
- Các đặc tính thiết yếu (Essential Characteristics)
- Các mô hình dịch vụ (Service Models)
- Các mô hình triển khai (Deployment Models)

Các đặc tính thiết yếu



Các đặc tính thiết yếu (tiếp)

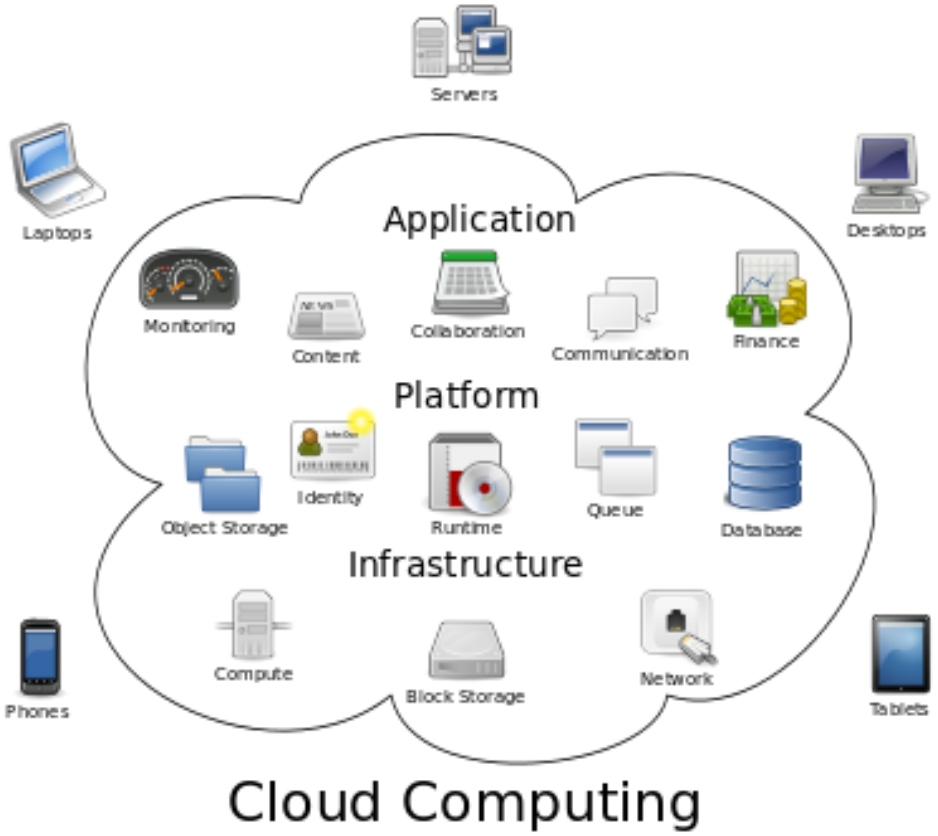
- On-demand self-service
  - Người sử dụng có thể cấp phát tài nguyên tính toán như thời gian máy chủ và khả năng lưu trữ một cách tự động mà không cần tương tác trực tiếp với nhà cung cấp dịch vụ.



Các đặc tính thiết yếu (tiếp)

❖ Broad Network Access

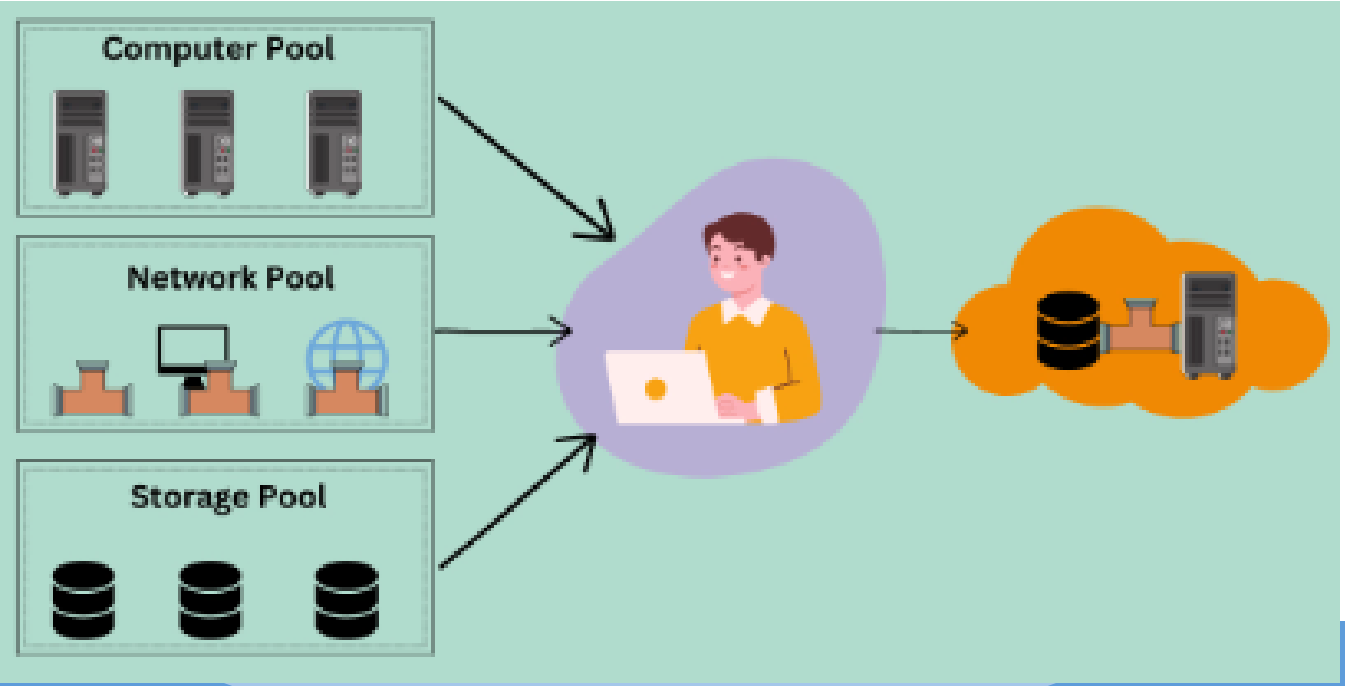
- Cung cấp khả năng truy nhập đến các tài nguyên tính toán đa dạng, với mọi loại phương tiện truyền dẫn và thiết bị đầu cuối;
- Hỗ trợ nhiều loại mạng: Ethernet, 3G, 4G, wifi,...
- Hỗ trợ nhiều thiết bị đầu cuối trên nhiều nền tảng khác nhau: Máy tính, điện thoại di động,...



Các đặc tính thiết yếu (tiếp)

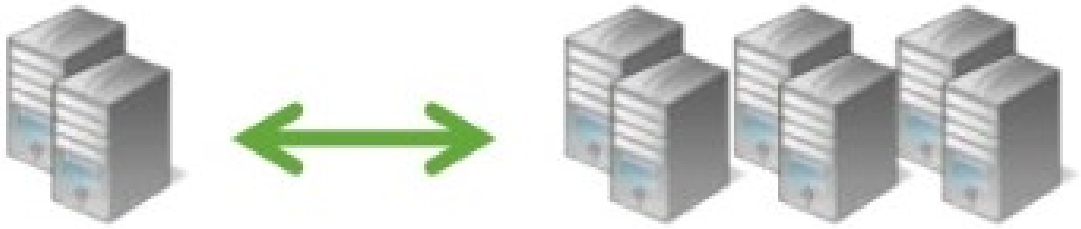
❖ Resource Pooling

- Tài nguyên máy tính của nhà cung cấp được gộp lại để phục vụ cho nhiều người dùng sử dụng một mô hình đa thuê bao, với các tài nguyên vật lý và ảo khác nhau được cấp phát động và cấp phát lại theo nhu cầu của người dùng.



Các đặc tính thiết yếu (tiếp)

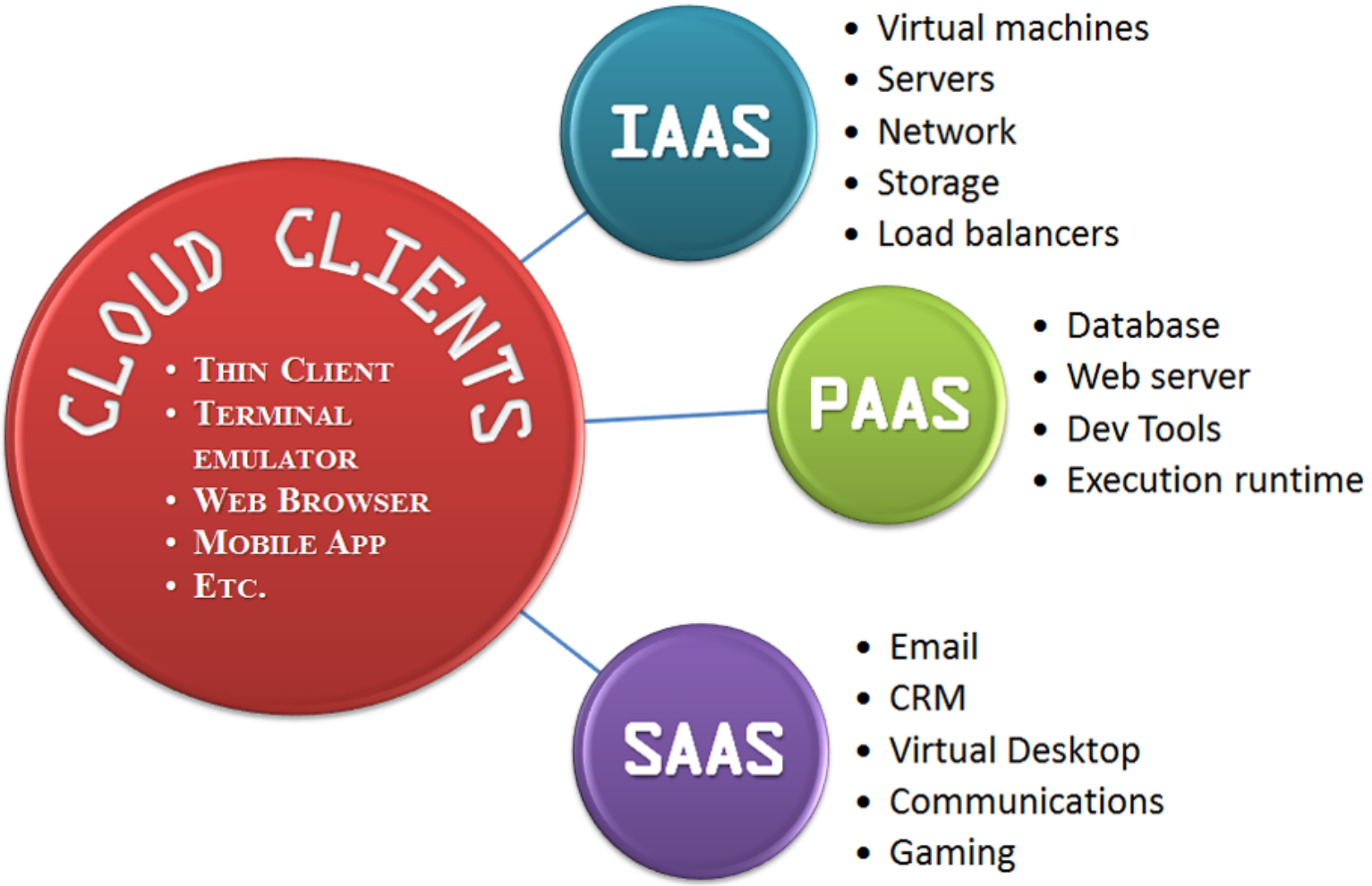
- Rapid elasticity
  - Các tài nguyên tính toán có thể được cấp phát nhanh chóng và 'co giãn' được. Có khả năng tăng hoặc giảm qui mô sử dụng tài nguyên một cách nhanh chóng, tự động theo yêu cầu;
  - Với người sử dụng, họ có thể đặt mua tài nguyên tính toán 'với bất kỳ số lượng nào và vào bất kỳ thời gian nào'.



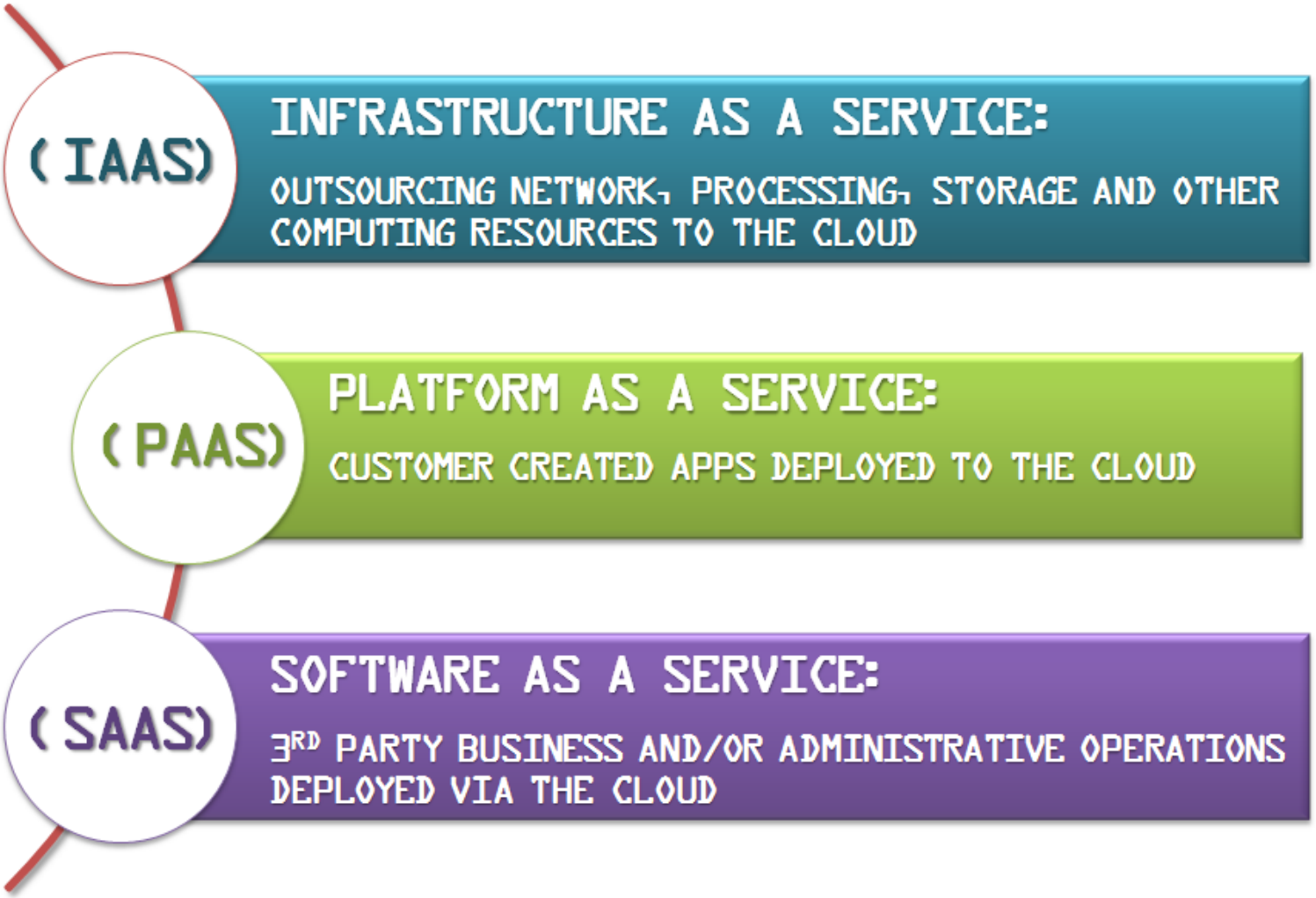
Các đặc tính thiết yếu (tiếp)

- Measured service
  - Hệ thống điện toán đám mây tự động kiểm soát và tối ưu hóa việc sử dụng tài nguyên bằng cách sử dụng khả năng đo kiểm ở một số mức độ trừu tượng thích hợp cho các loại hình dịch vụ;
  - Việc sử dụng tài nguyên có thể được giám sát, kiểm soát, và báo cáo – được cung cấp một cách minh bạch cho cả nhà cung cấp và người dùng của các dịch vụ

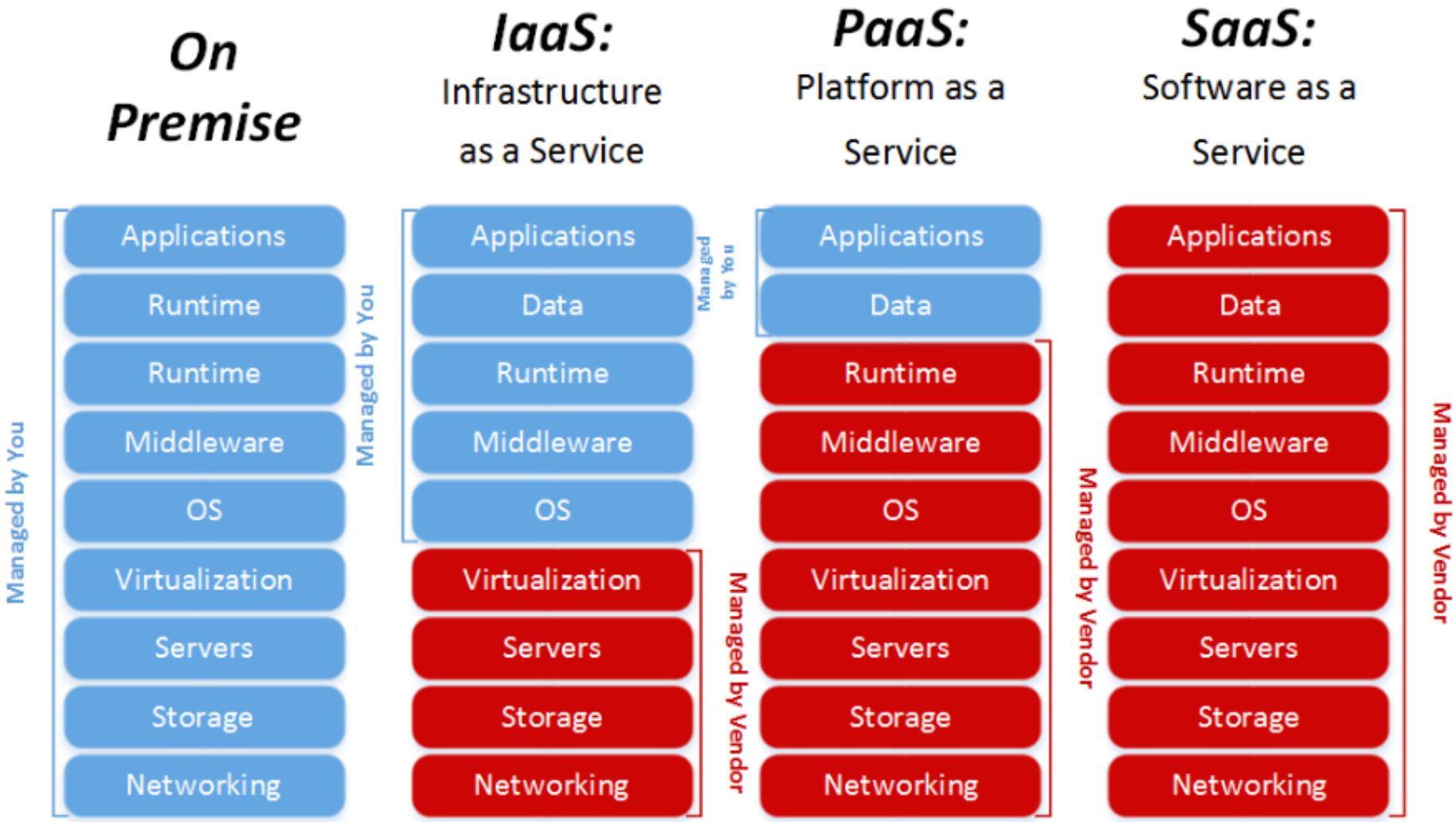
Các mô hình dịch vụ



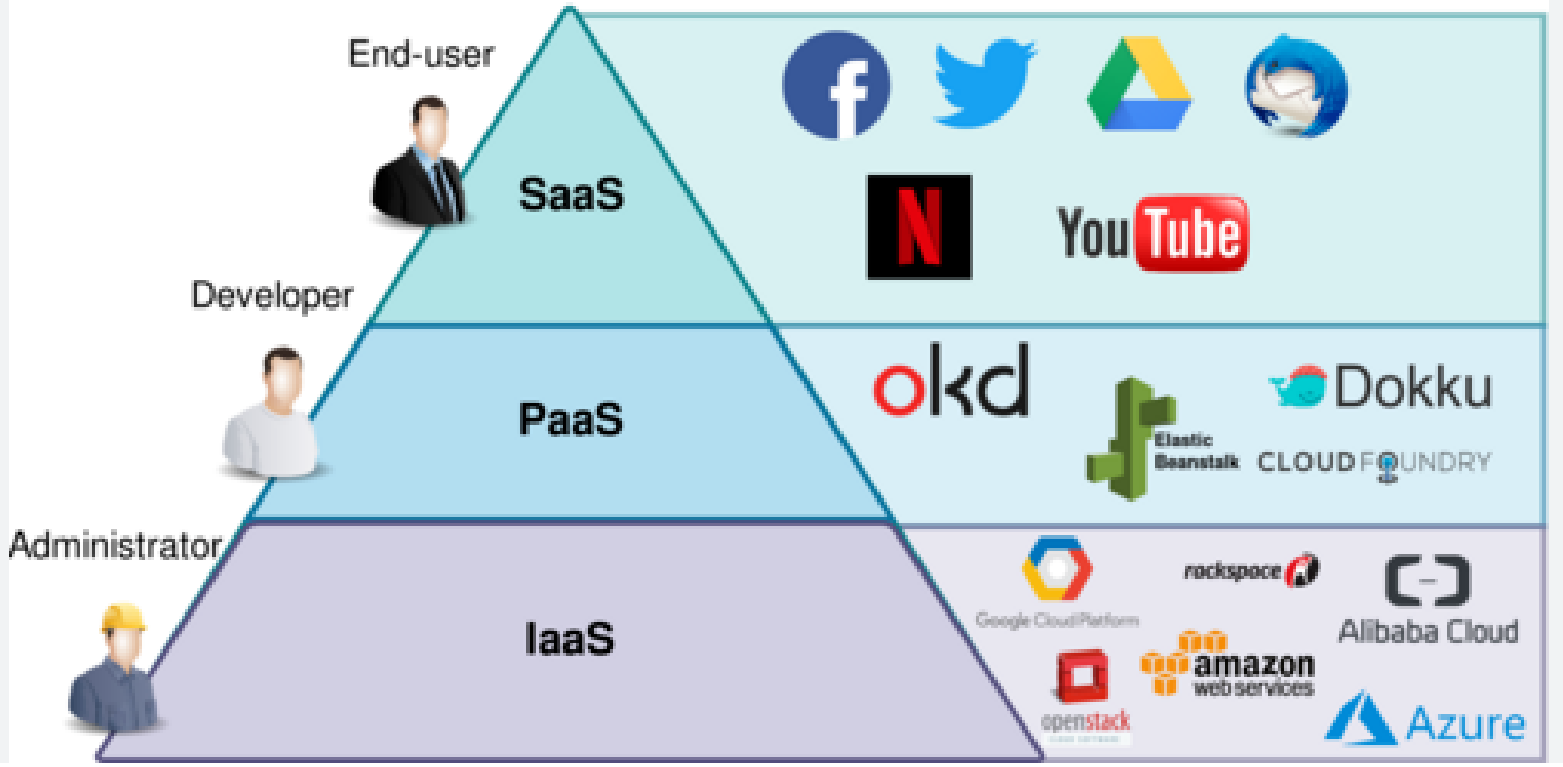
Các mô hình dịch vụ (tiếp)



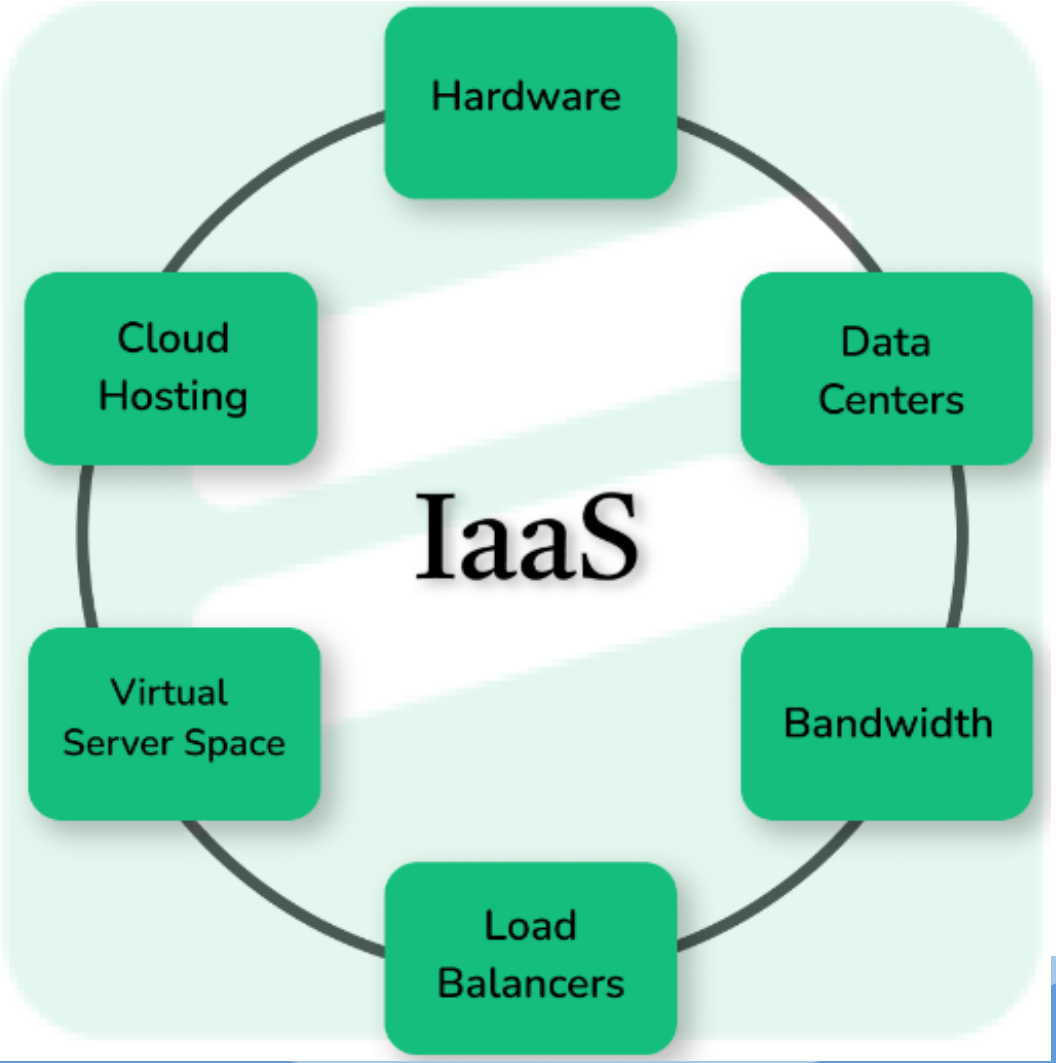
Các mô hình dịch vụ (tiếp)



Các mô hình dịch vụ (tiếp)



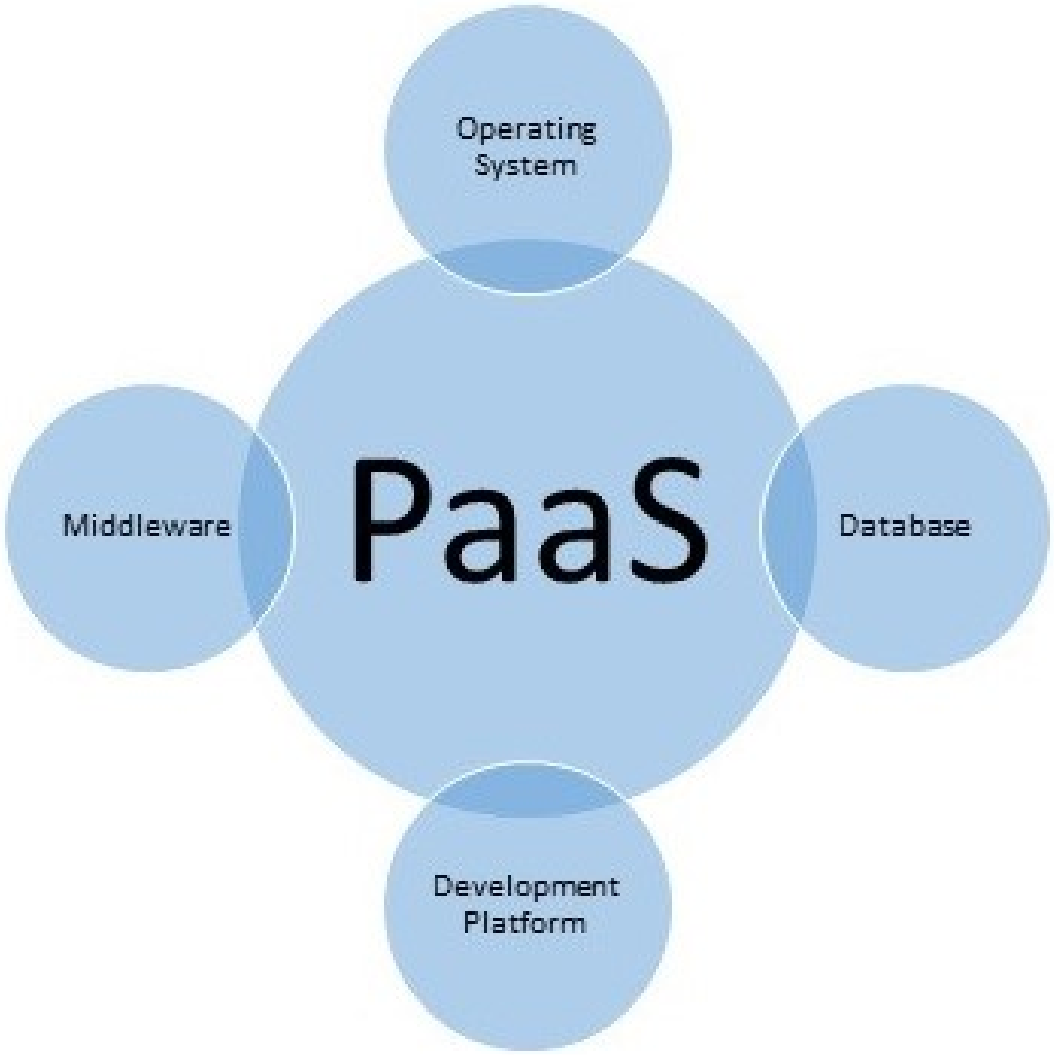
IaaS: Infrastructure as a Service – Hạ tầng như một dịch vụ



IaaS: Infrastructure as a Service – Hạ tầng như một dịch vụ

- Khách hàng có thể thuê kết nối mạng, năng lực xử lý, lưu trữ và các tài nguyên tính toán khác trên đám mây:
  - Có khả năng cung cấp cho khách hàng các tài nguyên tính toán như năng lực xử lý, lưu trữ, mạng và các tài nguyên khác;
  - Khách hàng có thể triển khai và chạy các phần mềm tùy ý, bao gồm cả hệ điều hành và các ứng dụng;
  - Khách hàng không được quản lý hoặc điều khiển hạ tầng đám mây, nhưng có khả năng điều khiển hệ điều hành, tiện tích lưu trữ, các ứng dụng đã cài đặt và có thể điều khiển một phần các thành phần mạng (như tường lửa cho host).

PaaS: Platform as a Service – Nền tảng như một dịch vụ



PaaS: Platform as a Service – Nền tảng như một dịch vụ

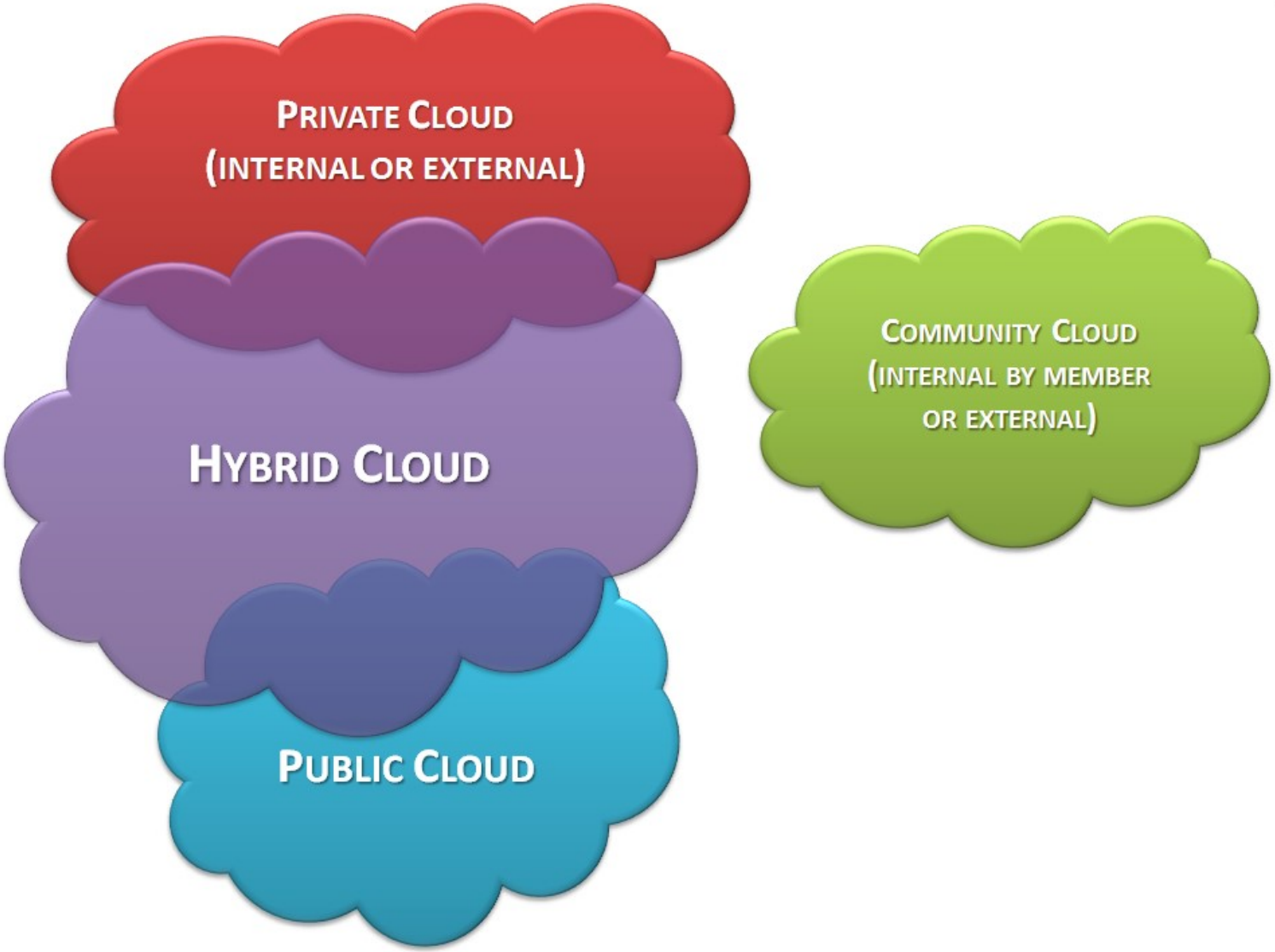
- Khách hàng có thể tạo các ứng dụng và triển khai lên đám mây:
  - Khách hàng được cung cấp khả năng triển khai các ứng dụng trên nền tảng đám mây đã mua/thuê sử dụng các ngôn ngữ lập trình và công cụ do nhà cung cấp dịch vụ hỗ trợ;
  - Khách hàng không được quản lý hoặc điều khiển hạ tầng đám mây, bao gồm mạng, máy chủ, hệ điều hành, khả năng lưu trữ, nhưng có thể điều khiển các ứng dụng đã triển khai, và có thể cả việc cấu hình môi trường hoạt động cho các ứng dụng.

SaaS: Software as a Service – Phần mềm như một dịch vụ

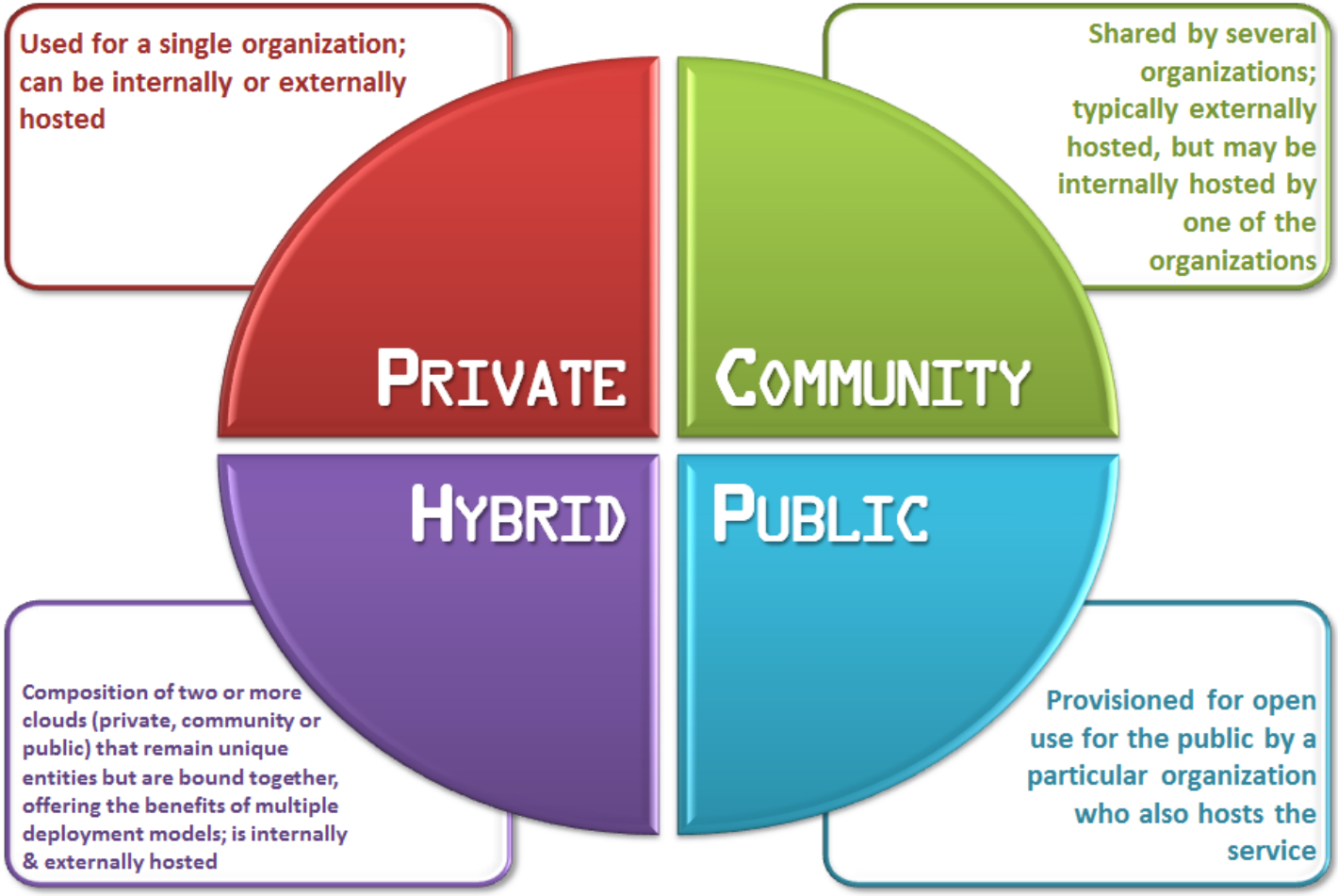
SaaS: Software as a Service – Phần mềm như một dịch vụ

- Khách hàng có thể thuê phần mềm của nhà cung cấp như 1 dịch vụ:
  - Khách hàng có thể thuê sử dụng các ứng dụng của nhà cung cấp triển khai trên hạ tầng đám mây;
  - Các ứng dụng có thể được truy nhập từ nhiều máy khách khác nhau thông qua một giao diện máy khách 'gầy' (thin client), như là 1 trình duyệt (VD: 1 web-based email);
  - Khách hàng không được quản lý hoặc điều khiển hạ tầng đám mây, bao gồm mạng, máy chủ, hệ điều hành, khả năng lưu trữ, hoặc thậm chí tính năng của từng ứng dụng. Tuy nhiên, họ có thể điều khiển hạn chế các cài đặt cấu hình ứng dụng của người dùng.

Mô hình triển khai các đám mây



Mô hình triển khai các đám mây (tiếp)



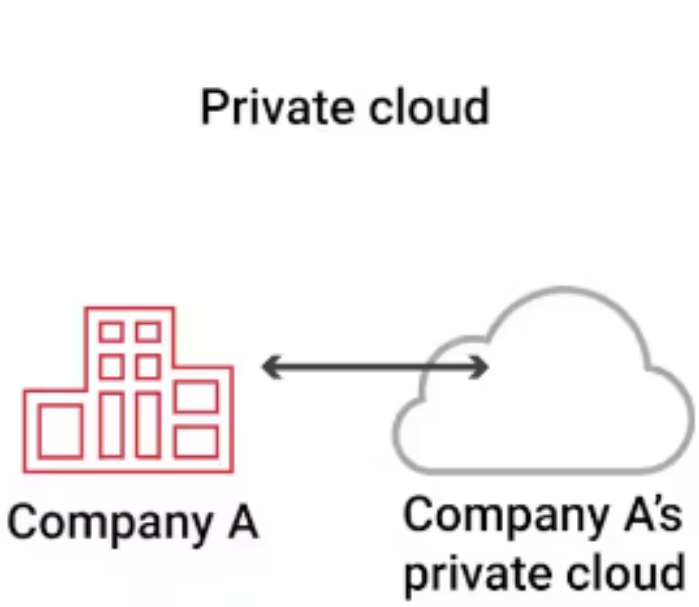
Mô hình triển khai các đám mây (tiếp)

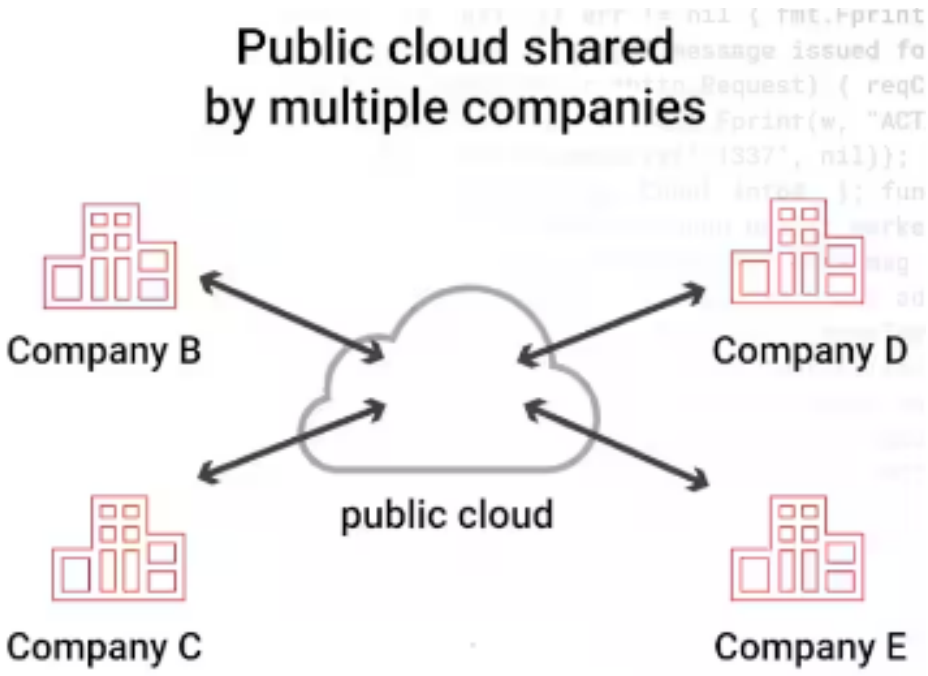
- Public Cloud (Đám mây công cộng):
  - Hạ tầng đám mây được cung cấp rộng rãi cho công chúng, hoặc một tập đoàn công nghiệp lớn;
  - Sở hữu bởi một tổ chức cung cấp dịch vụ điện toán đám mây.

Mô hình triển khai các đám mây (tiếp)

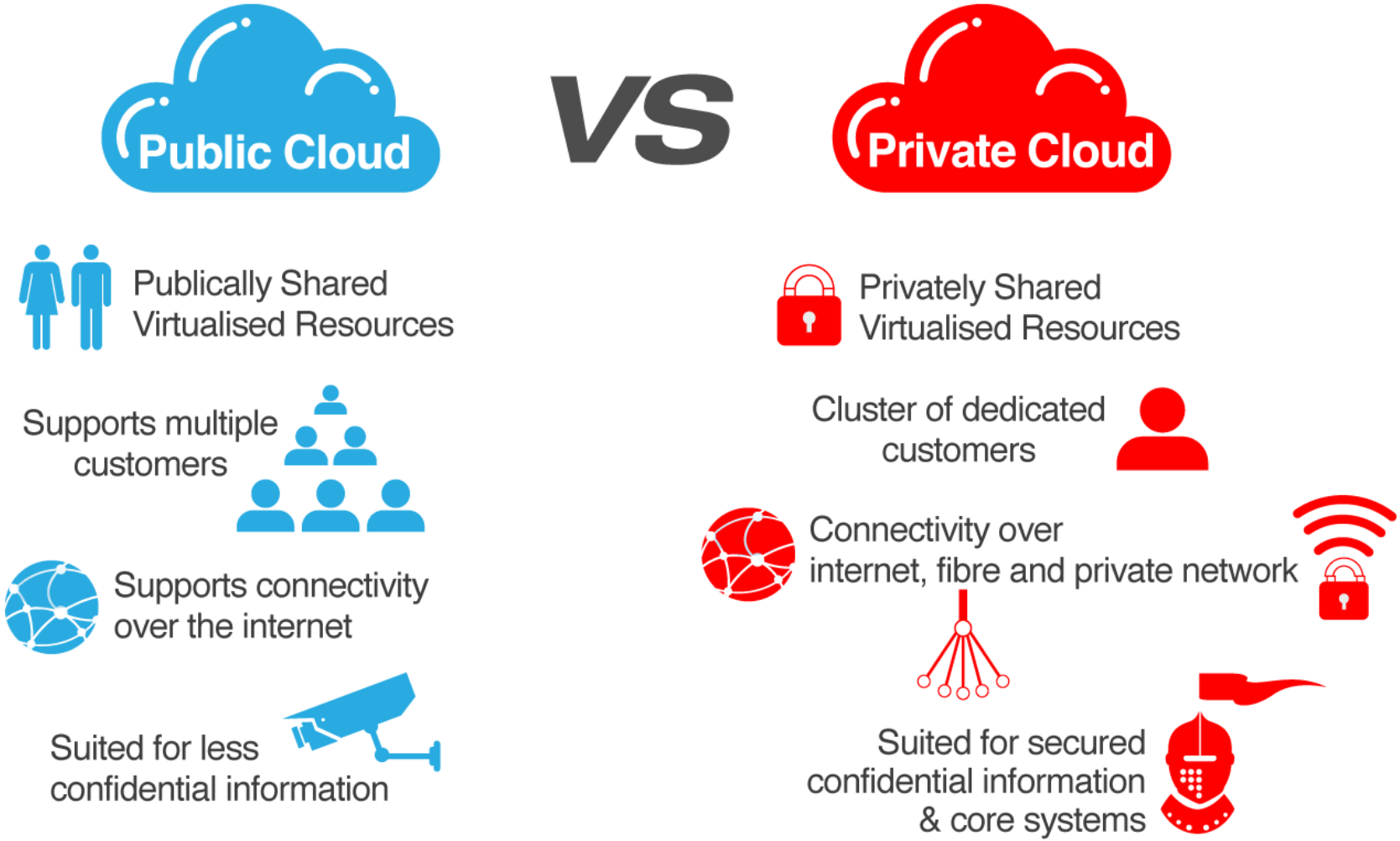
- Private Cloud (Đám mây riêng):
  - Hạ tầng đám mây được vận hành chỉ cho một tổ chức duy nhất;
  - Có thể được quản lý bởi tổ chức đó hoặc 1 bên thứ 3;
  - Có thể được host tại chỗ hoặc ở bên ngoài.

Mô hình triển khai các đám mây (tiếp)



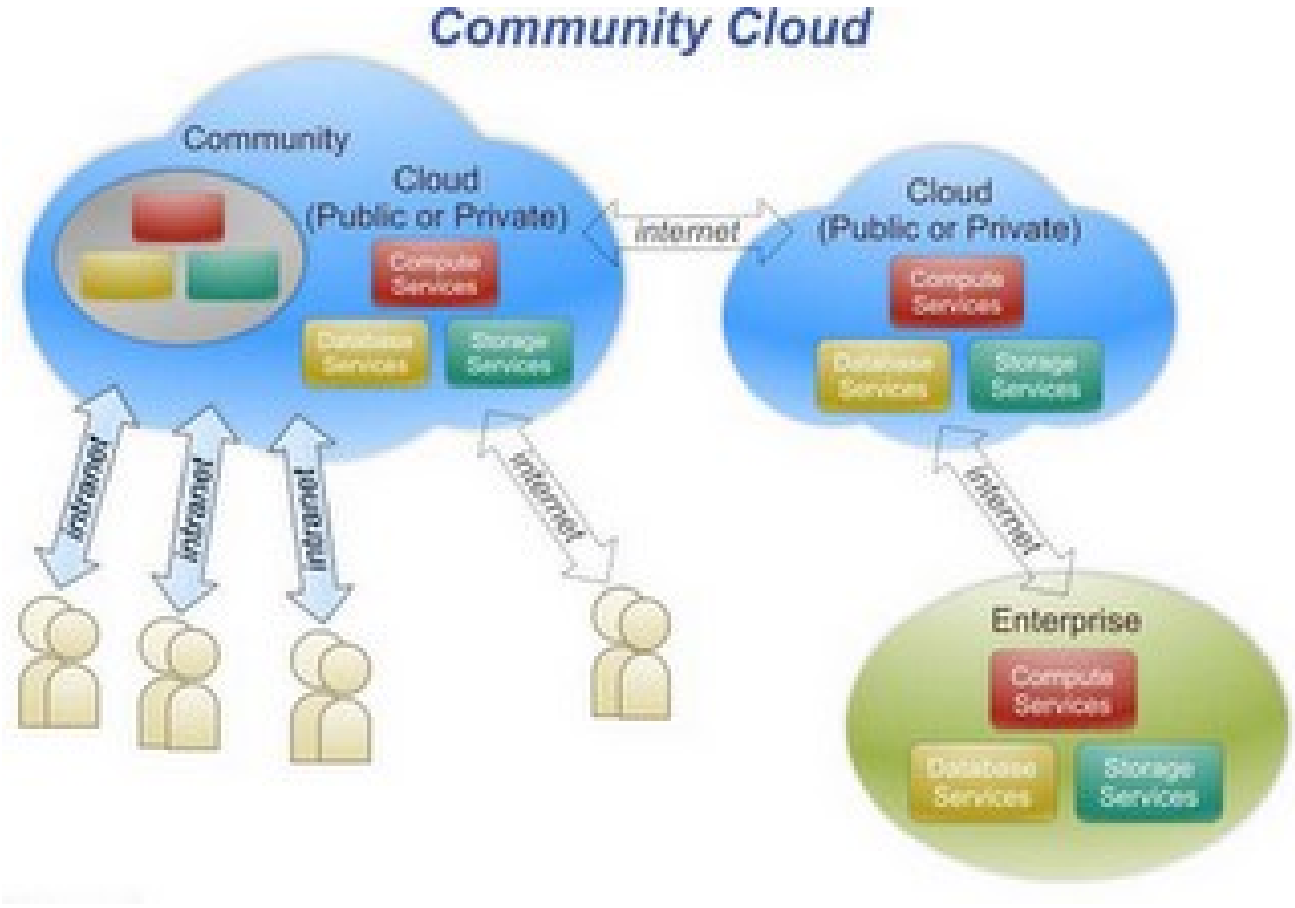


Mô hình triển khai các đám mây (tiếp)



Mô hình triển khai các đám mây (tiếp)

❖ Community Cloud (Đám mây cộng đồng):

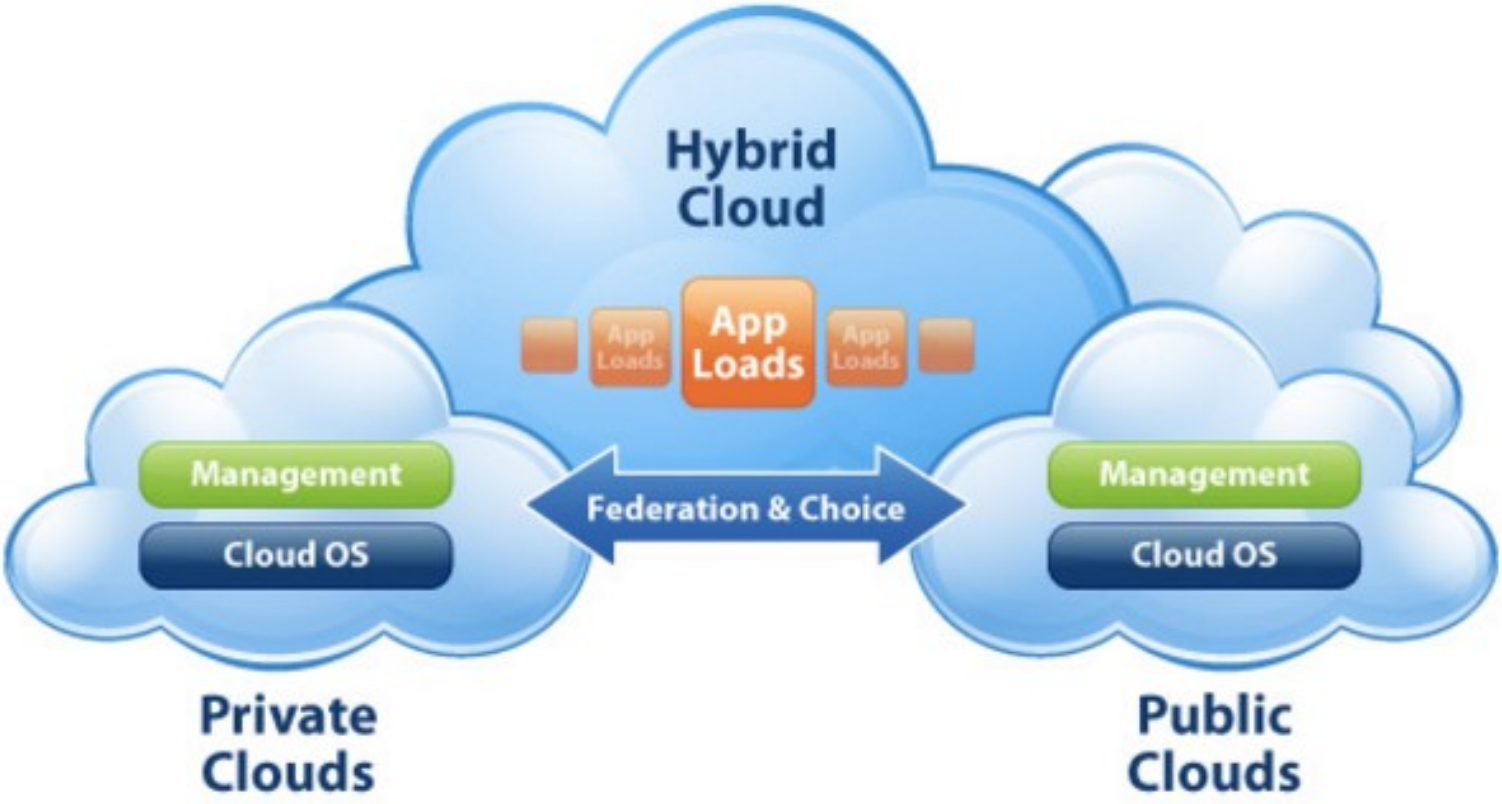


Mô hình triển khai các đám mây (tiếp)

- Community Cloud (Đám mây cộng đồng):
  - Hạ tầng đám mây được chia sẻ bởi nhiều tổ chức;
  - Hỗ trợ một cộng đồng có cùng các mối quan tâm (như sứ mệnh, yêu cầu an ninh, chính sách, ...);
  - Có thể được quản lý bởi các tổ chức đó hoặc 1 bên thứ 3;
  - Có thể được host tại chỗ hoặc ở bên ngoài.

Mô hình triển khai các đám mây (tiếp)

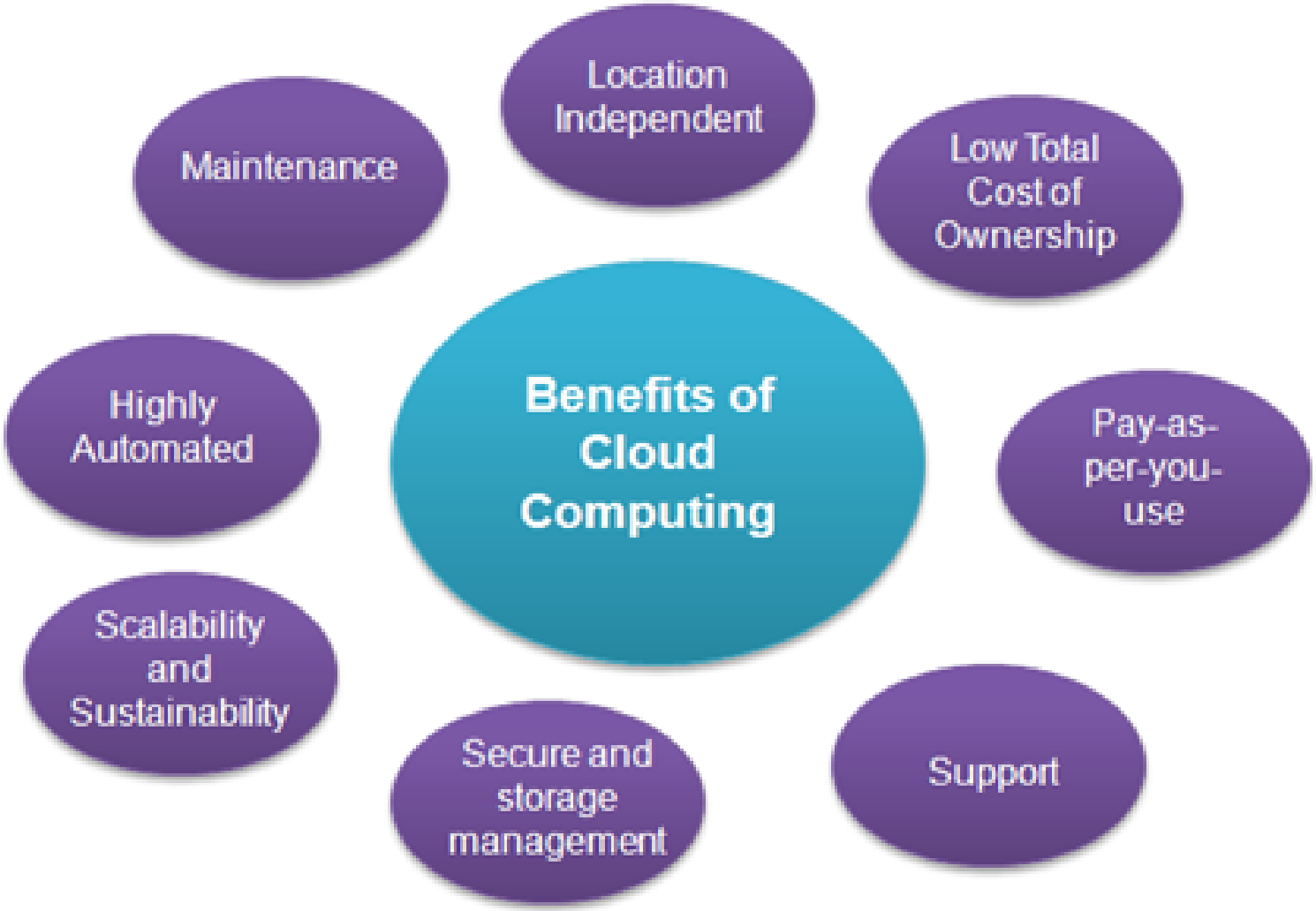
❖ Hybrid Cloud (Đám mây lai):



Mô hình triển khai các đám mây (tiếp)

- Hybrid Cloud (Đám mây lai):
  - Hạ tầng đám mây là sự kết hợp của 2 hay nhiều đám mây (đám mây riêng, công cộng, hoặc cộng đồng);
  - Các đám mây thành viên vẫn là các thực thể riêng, nhưng được liên kết thông qua công nghệ chuẩn hoặc độc quyền, cho phép dữ liệu và ứng dụng khả chuyển (ví dụ: Bùng nổ đám mây (Cloud Bursting) cho cân bằng tải giữa các đám mây).
    - Cloud Bursting: Khi ta đang sử dụng 1 đám mây cục bộ mà cần thêm tài nguyên có thể 'bùng nổ' chuyển sang đám mấy công cộng với nhiều tài nguyên tính toán hơn.

4.3 Lợi ích của điện toán đám mây



4.3 Lợi ích của điện toán đám mây

- Location independence: Tài nguyên tính toán được cung cấp độc lập về vị trí (mọi lúc, mọi nơi)
- Low total cost of ownership: Tổng chi phí sở hữu rẻ
- Support: Hỗ trợ tốt
- Secure and storage management: Quản lý lưu trữ và bảo mật
- Scalabilty and sustainability: Khả năng mở rộng và bền vững
- Highly automated: Tự động hóa cao (người dùng có thể đăng ký sử dụng tài nguyên hoàn toàn tự động)
- Maintenance: Bảo trì tốt.

Các hạn chế của điện toán đám mây

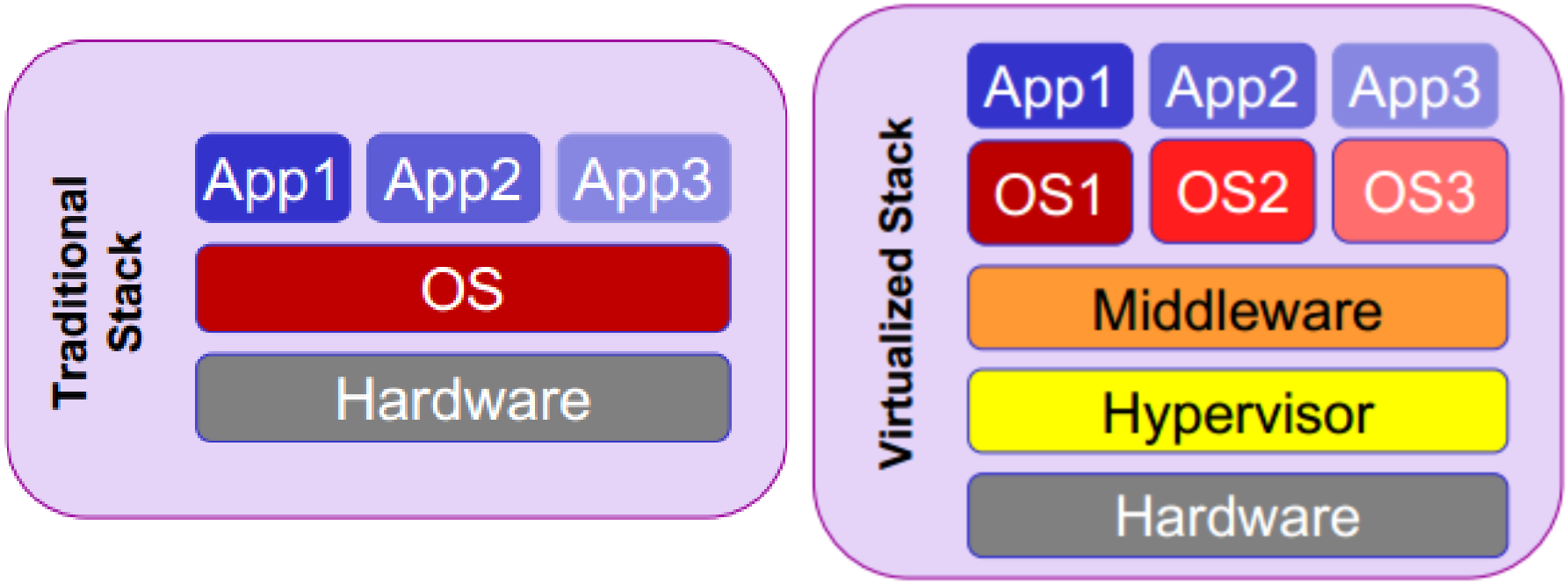
- Luôn yêu cầu phải có kết nối Internet;
- Làm việc không hiệu quả với kết nối Internet tốc độ chậm;
- Có thể có hạn chế về tính năng;
- Hiệu năng có thể thấp;
- Dữ liệu lưu trữ có thể không an toàn;
- Dữ liệu lưu trữ có thể bị mất;
- Vấn đề tương thích giữa các đám mây.

4.4 Các công nghệ nền tảng xây dựng ĐTĐM

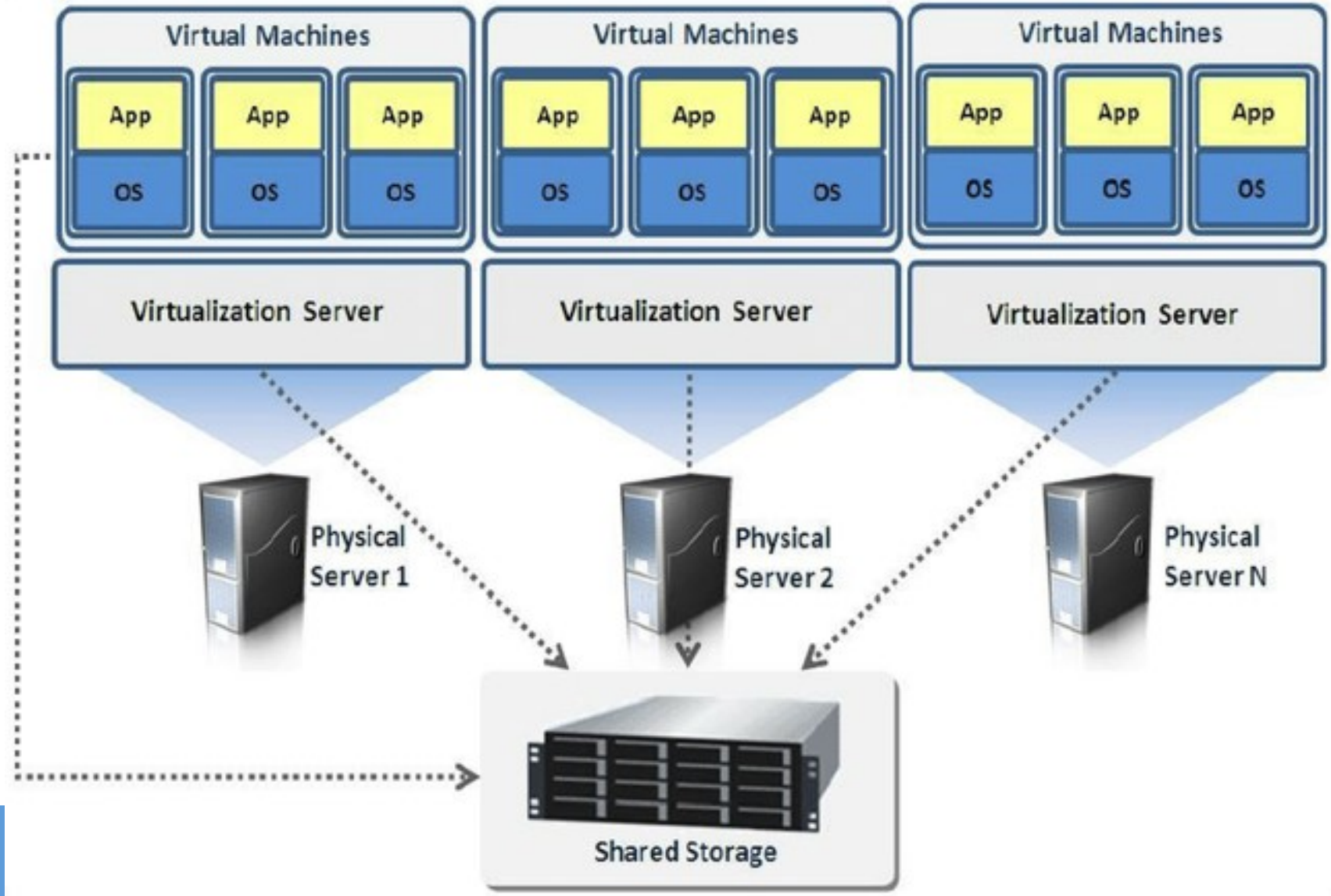
- Virtualization
- Web 2.0
- Distributed Storage
- Distributed Computing
- Utility Computing
- Network Bandwidth & Latency
- Fault-Tolerant Systems

Công nghệ nền tảng: Ảo hóa

- Ảo hóa cho phép chia sẻ các tài nguyên tính toán: máy chủ, dữ liệu, mạng, phần mềm và CSDL.

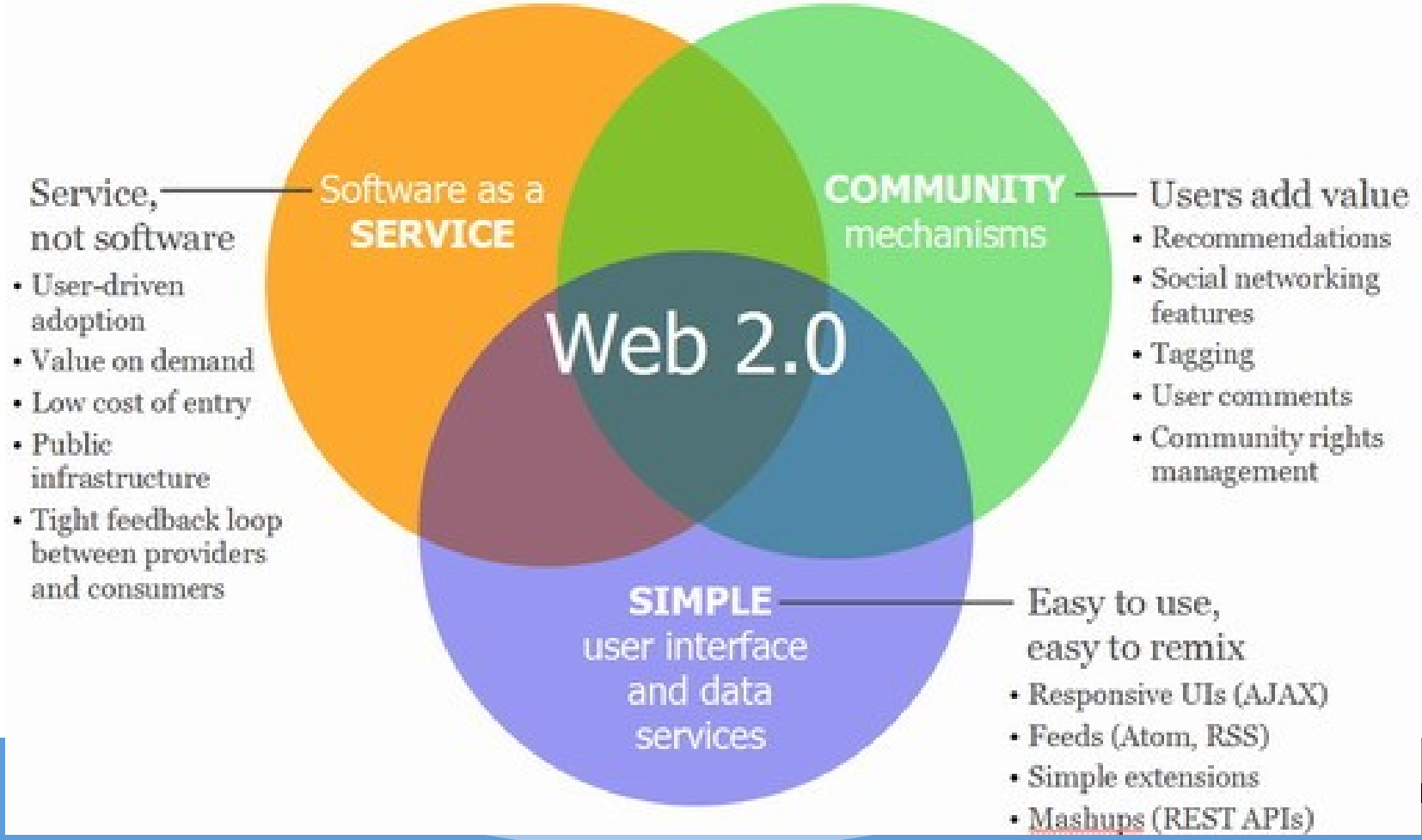


Công nghệ nền tảng: Ảo hóa



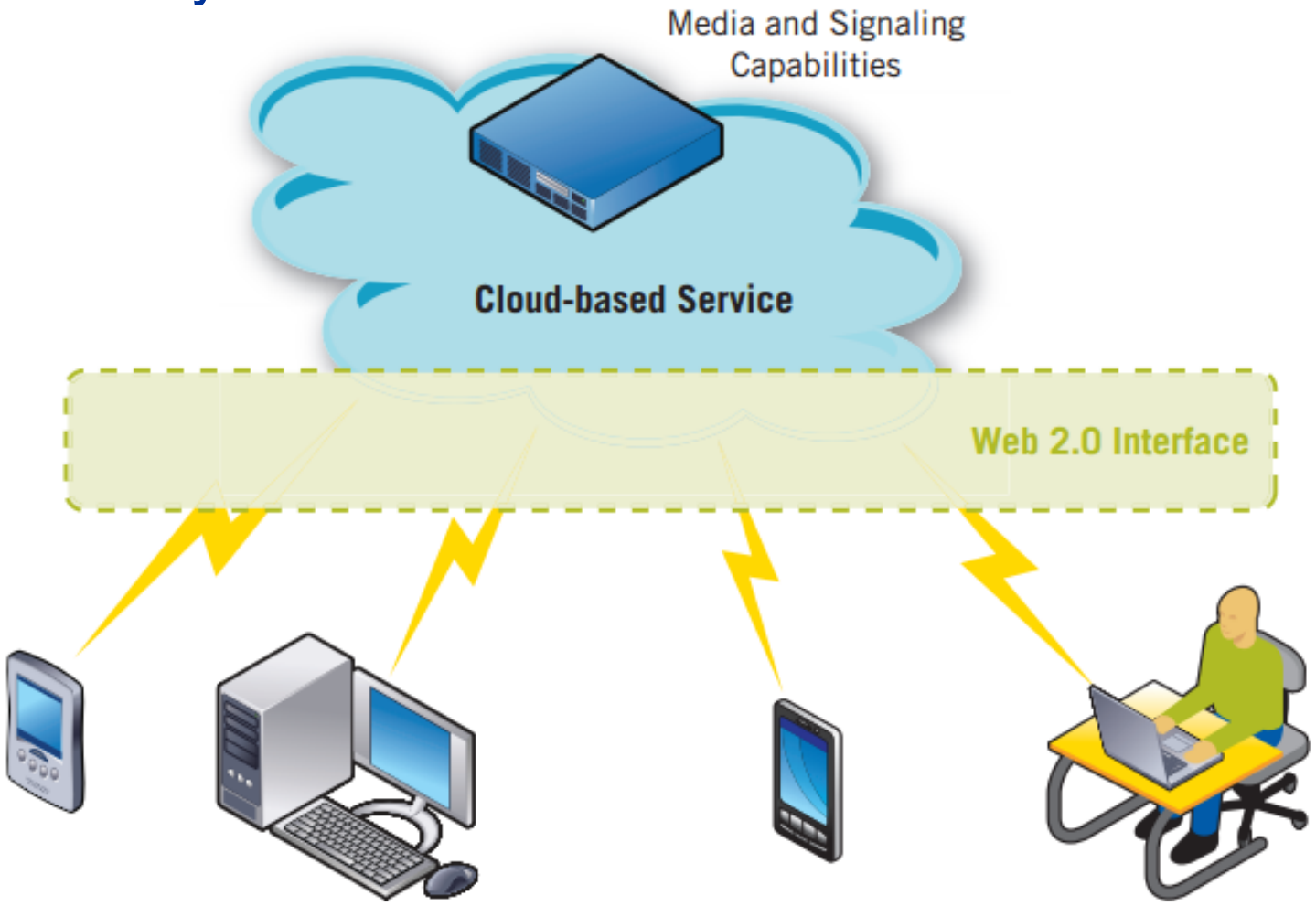
Công nghệ nền tảng: Web 2.0

- Web 2.0 là nền tảng mới cho phép ứng dụng web tăng tính tương tác và phối hợp/hội tụ.

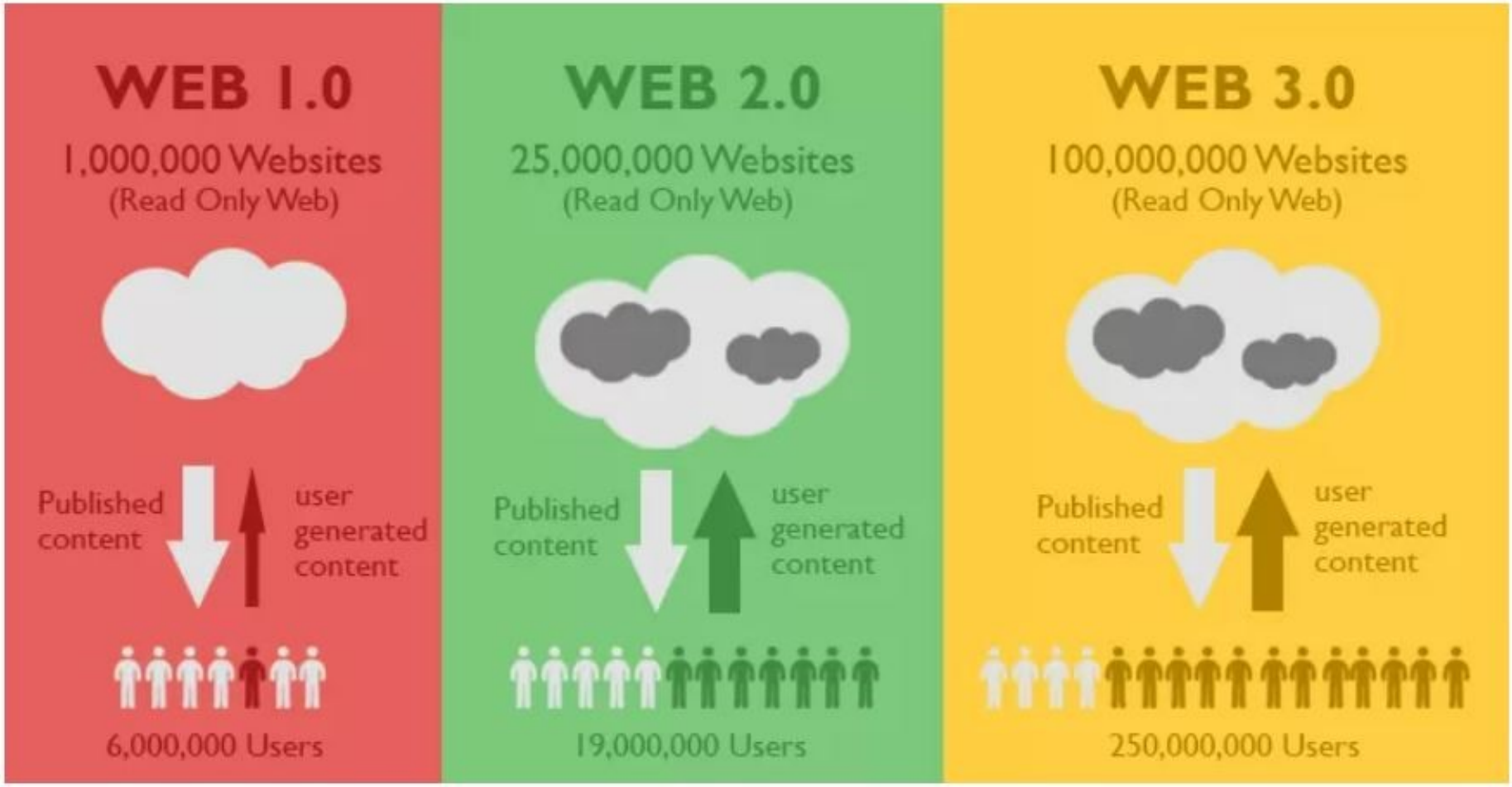


Công nghệ nền tảng: Web 2.0

- Web 2.0 là một trong các giao diện cho các máy khách truy nhập đám mây.

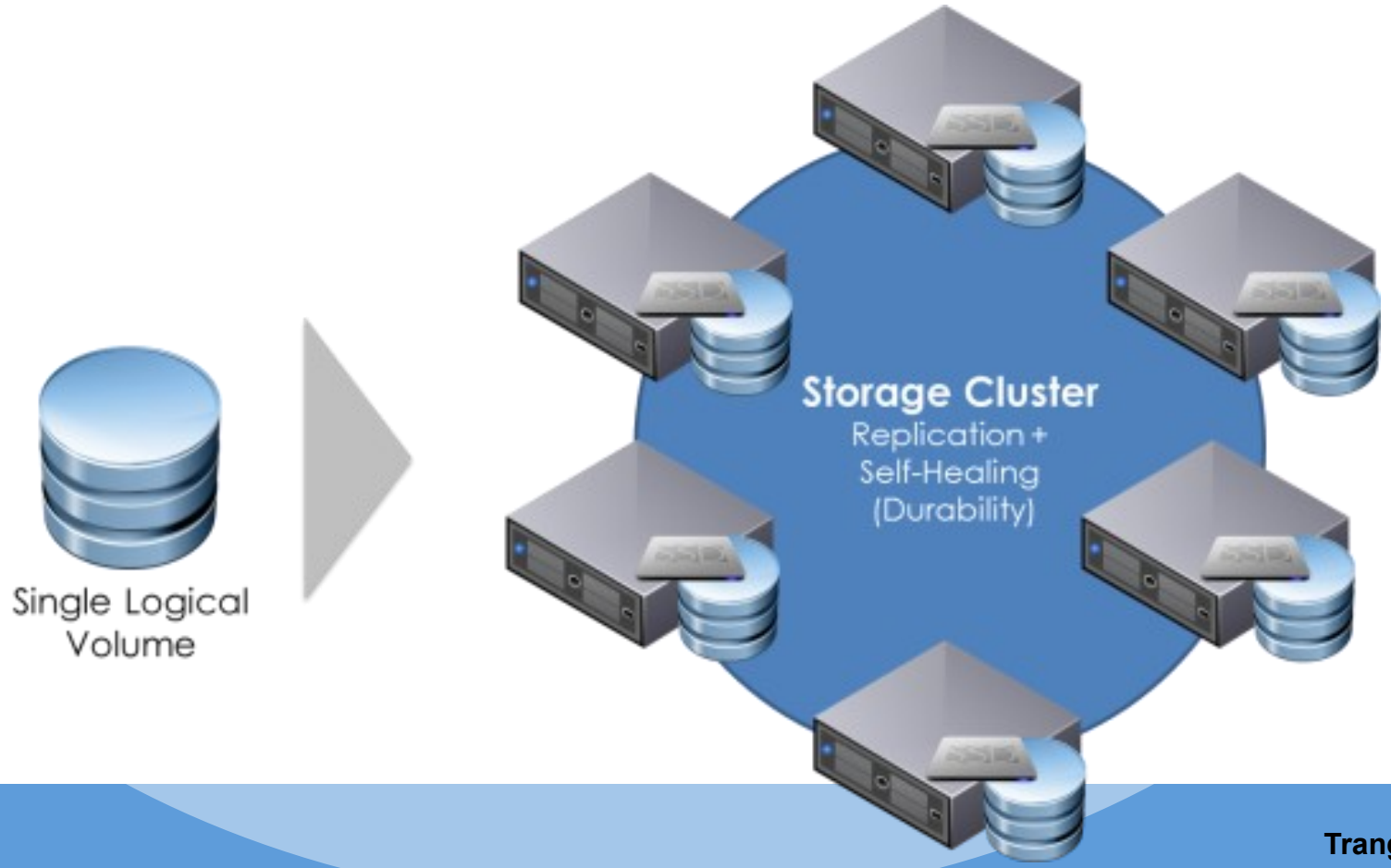


Công nghệ nền tảng: Web 2.0



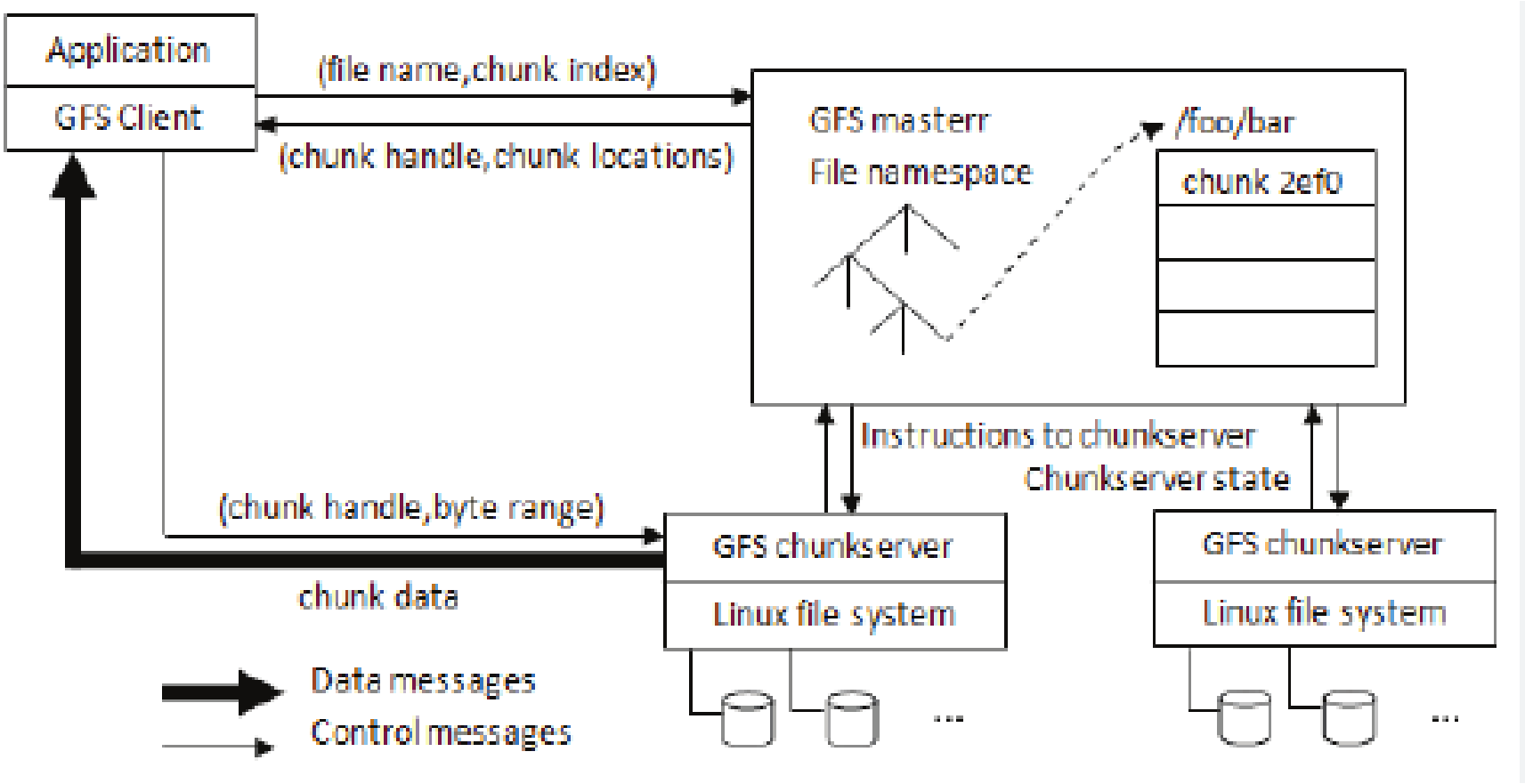
Công nghệ nền tảng: Distributed Storage

- Distributed Storage: DFS/SAN cung cấp dung lượng lớn với độ an toàn cao, tốc độ cao.



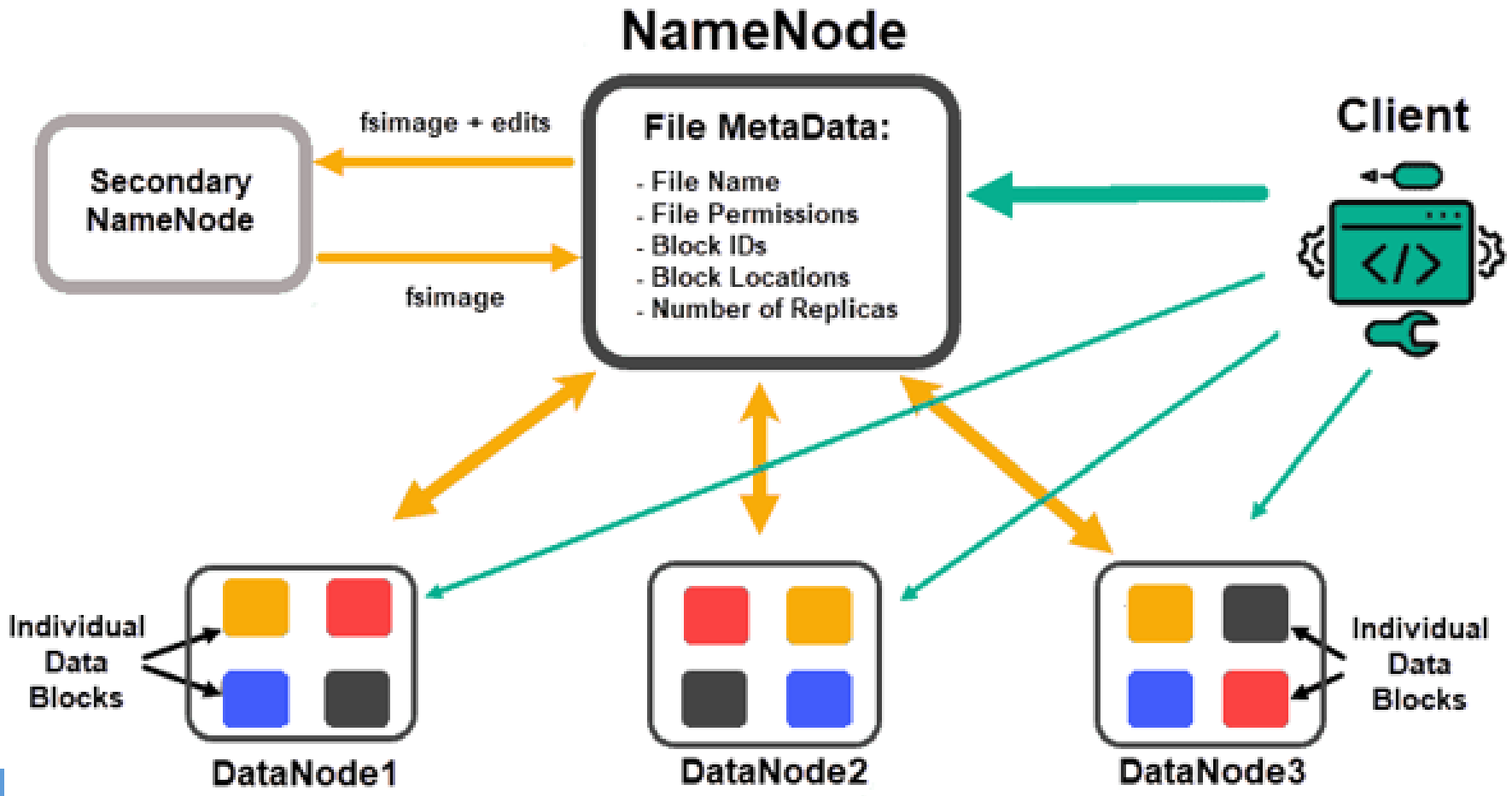
Công nghệ nền tảng: Distributed Storage

❖ Google Distributed File System:

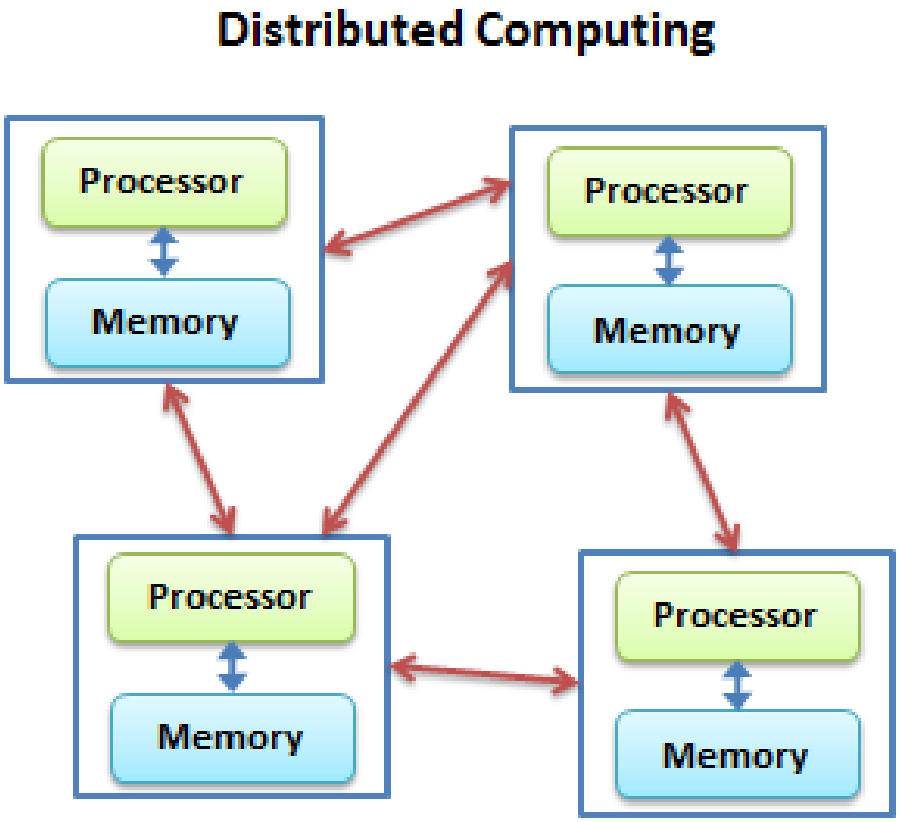


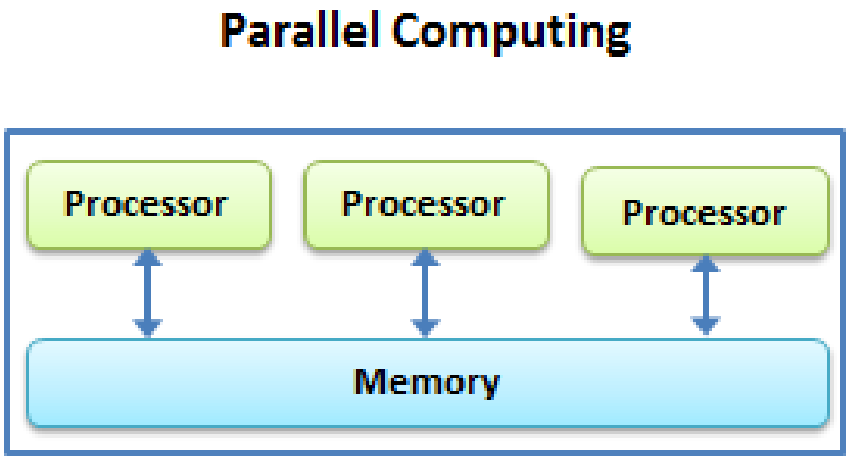
Công nghệ nền tảng: Distributed Storage

❖ Hadoop Distributed File System:

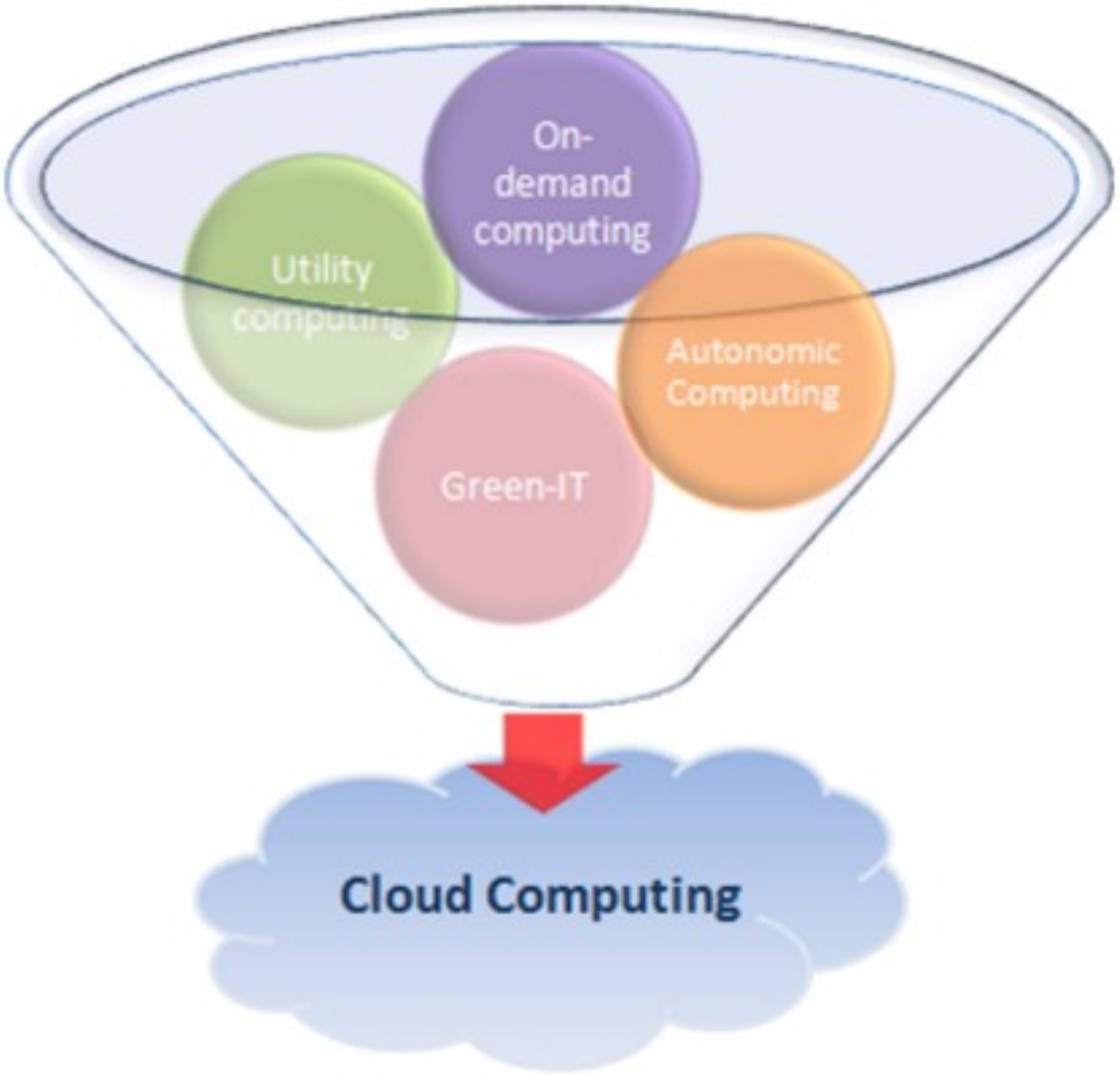


Công nghệ nền tảng: Distributed Computing





Công nghệ nền tảng: Utility Computing



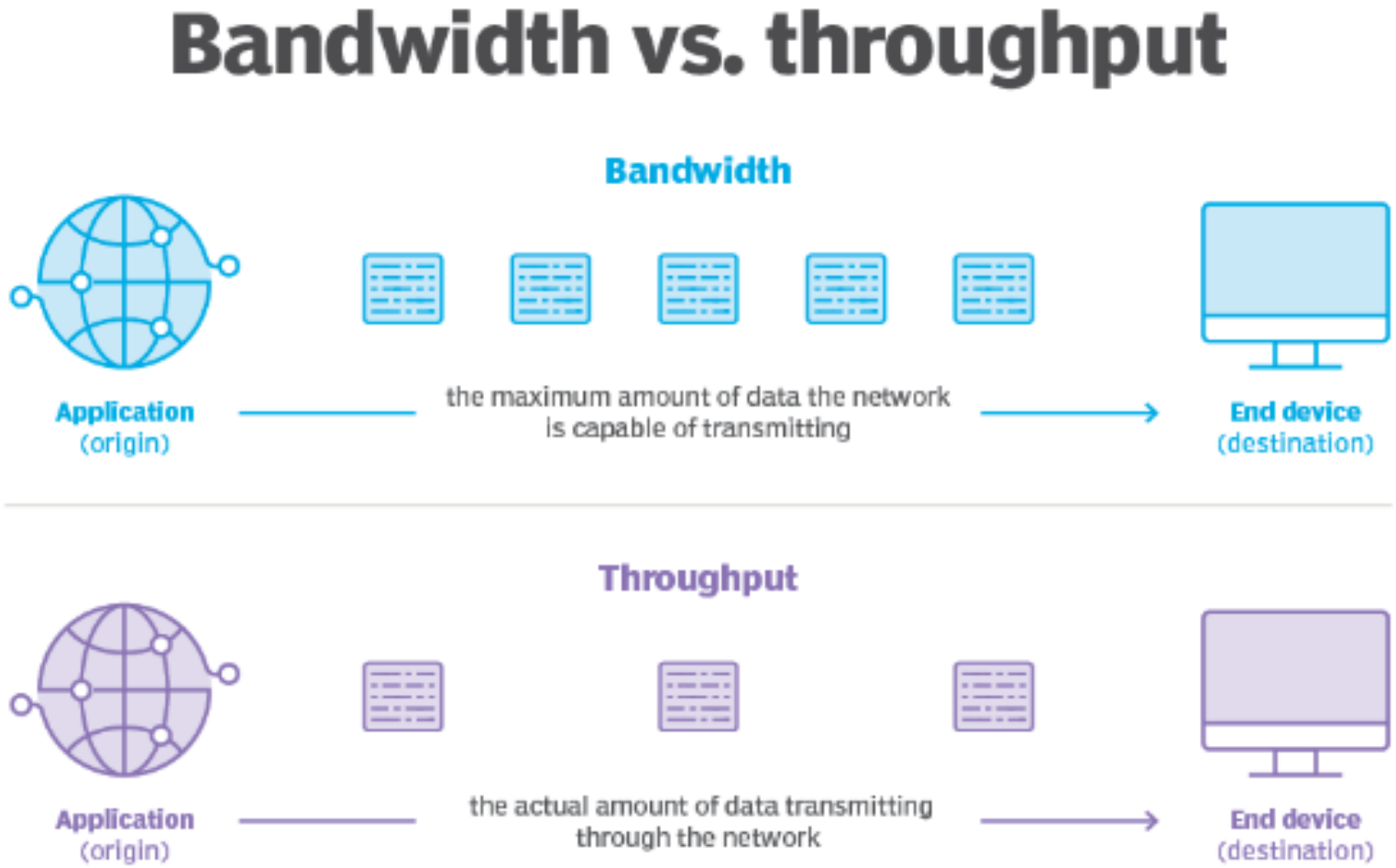
Công nghệ nền tảng: Utility Computing

- Utility Computing (Điện toán tiện ích) là một mô hình dịch vụ nhằm cung cấp các tài nguyên tính toán, như phần cứng, phần mềm và băng thông mạng cho khách hàng khi họ có yêu cầu;
  - Khách hàng chỉ phải thanh toán phí dịch vụ theo lượng sử dụng (pay as you go) mà không phải trả khoản phí cố định, hoặc mức giá cố định.
  - Điện toán tiện ích là một tập hợp con của điện toán đám mây, cho phép người dùng mở rộng quy mô dựa trên nhu cầu của họ.
    - Khách hàng, người dùng hoặc doanh nghiệp có được các tiện ích như không gian lưu trữ dữ liệu, khả năng tính toán, dịch vụ ứng dụng, máy chủ ảo hoặc thậm chí cho thuê phần cứng như CPU, màn hình và thiết bị đầu vào.

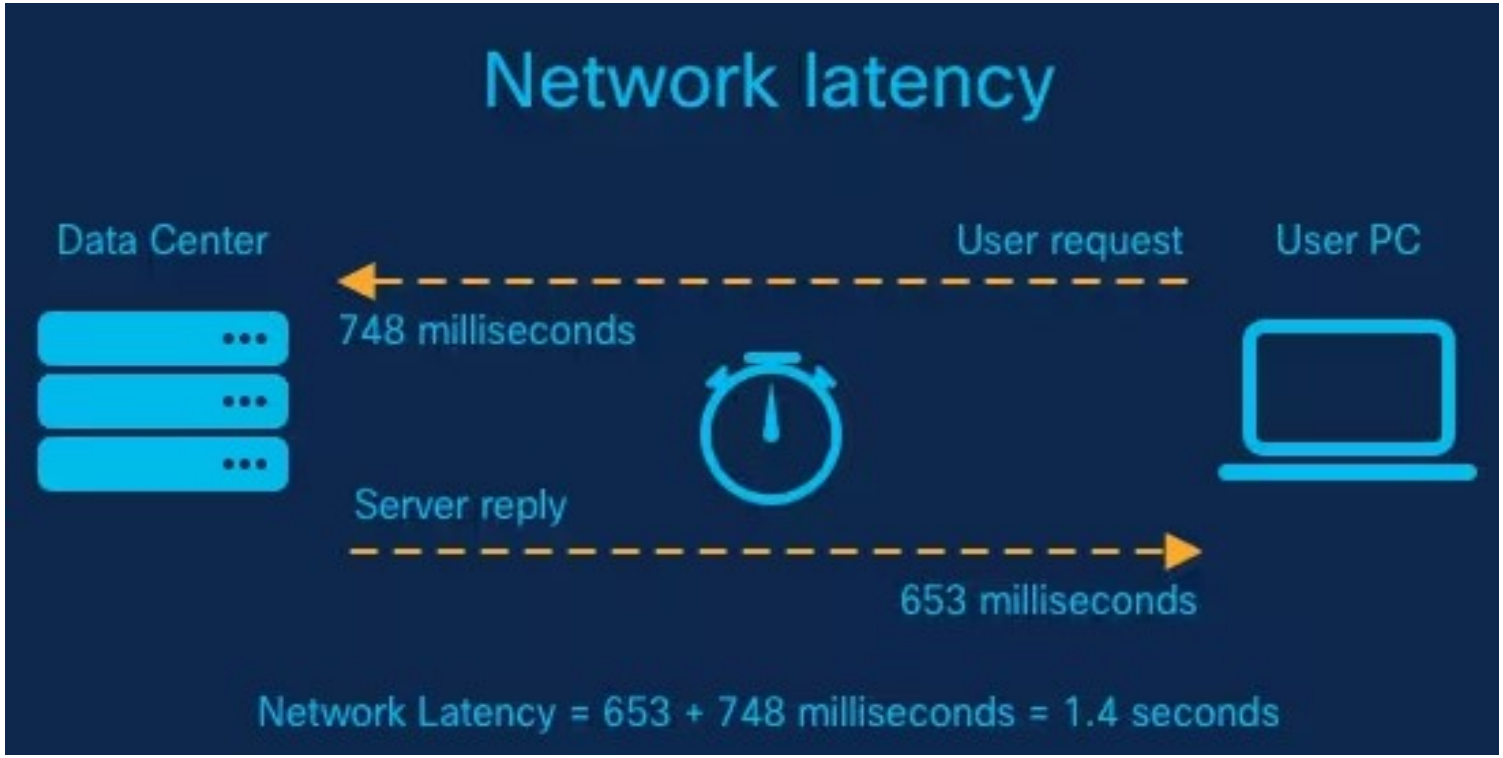
Công nghệ nền tảng: Network Bandwidth & Latency

- Network Bandwidth (Băng thông mạng): năng lực vận chuyển của mạng.
  - Càng lớn càng tốt.
- Network Latency (Độ trễ mạng): thời gian để 1 gói tin đi từ điểm này đến 1 điểm khác trong mạng;
  - Càng nhỏ càng tốt.

Công nghệ nền tảng: Network Bandwidth & Latency

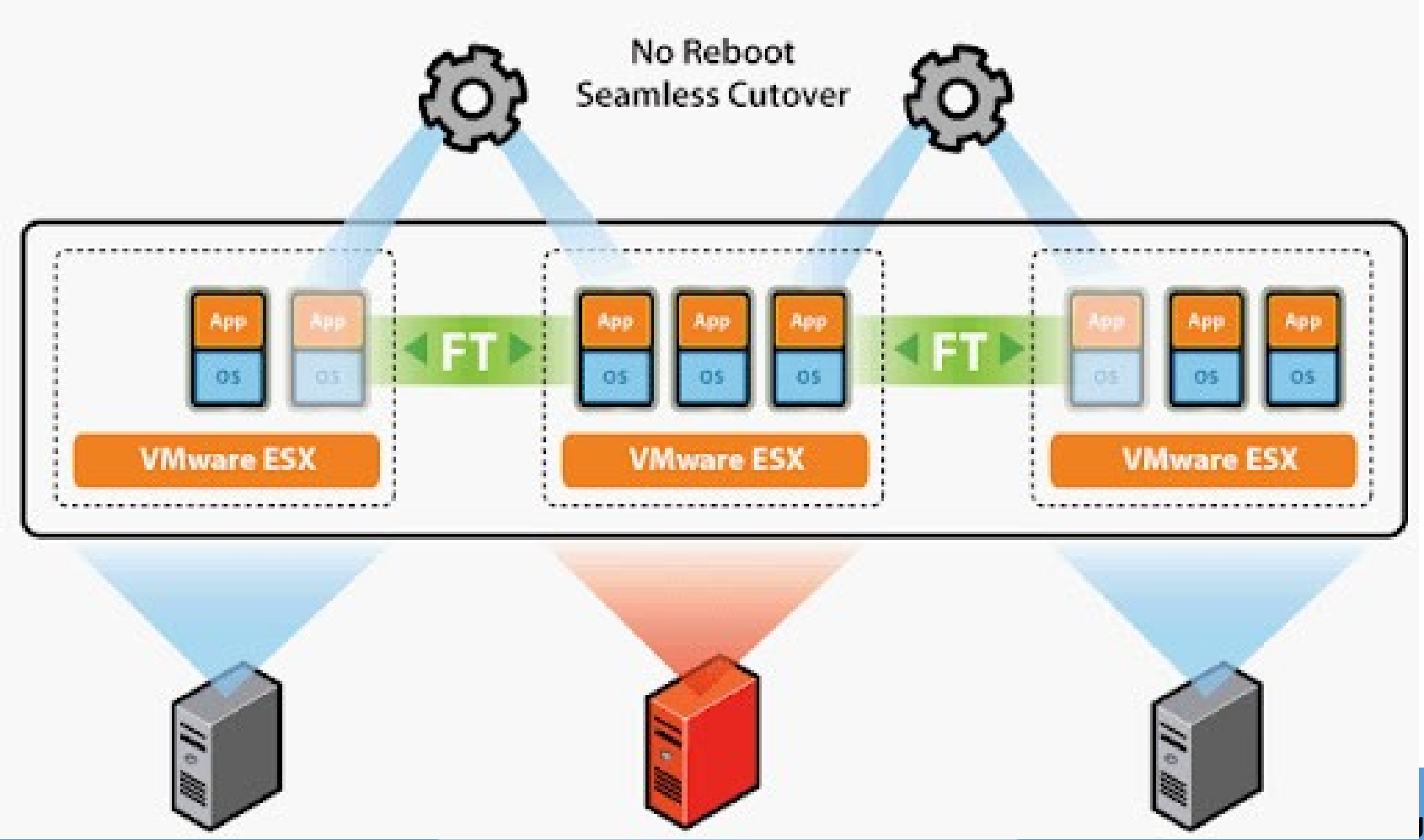


Công nghệ nền tảng: Network Bandwidth & Latency



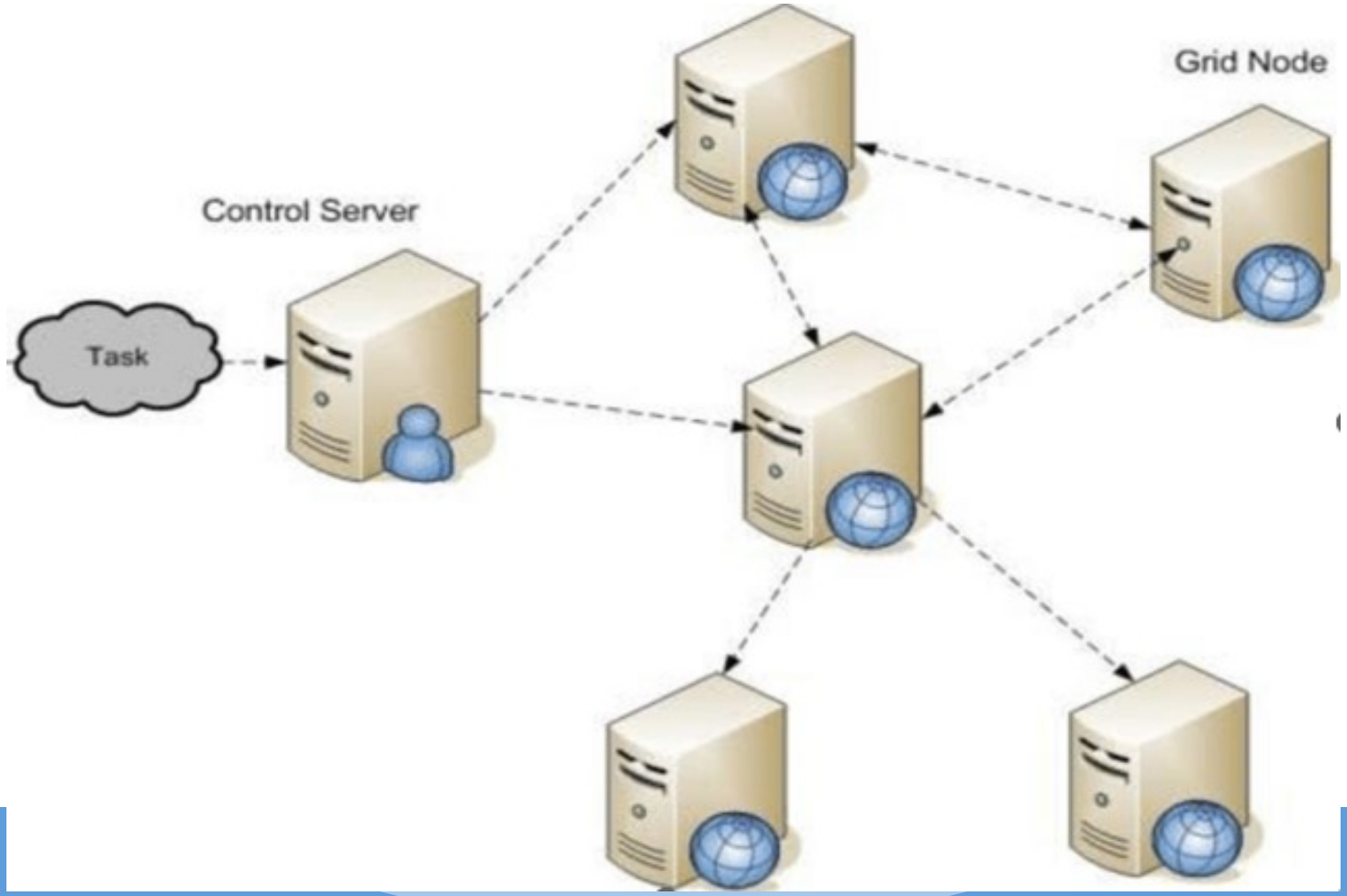
Công nghệ nền tảng: Fault-Tolerant Systems

❖ Fault-Tolerant Systems (Các hệ thống có khả năng chịu lỗi)



4.5 Tính toán lưới (Grid Computing) và ĐTĐM

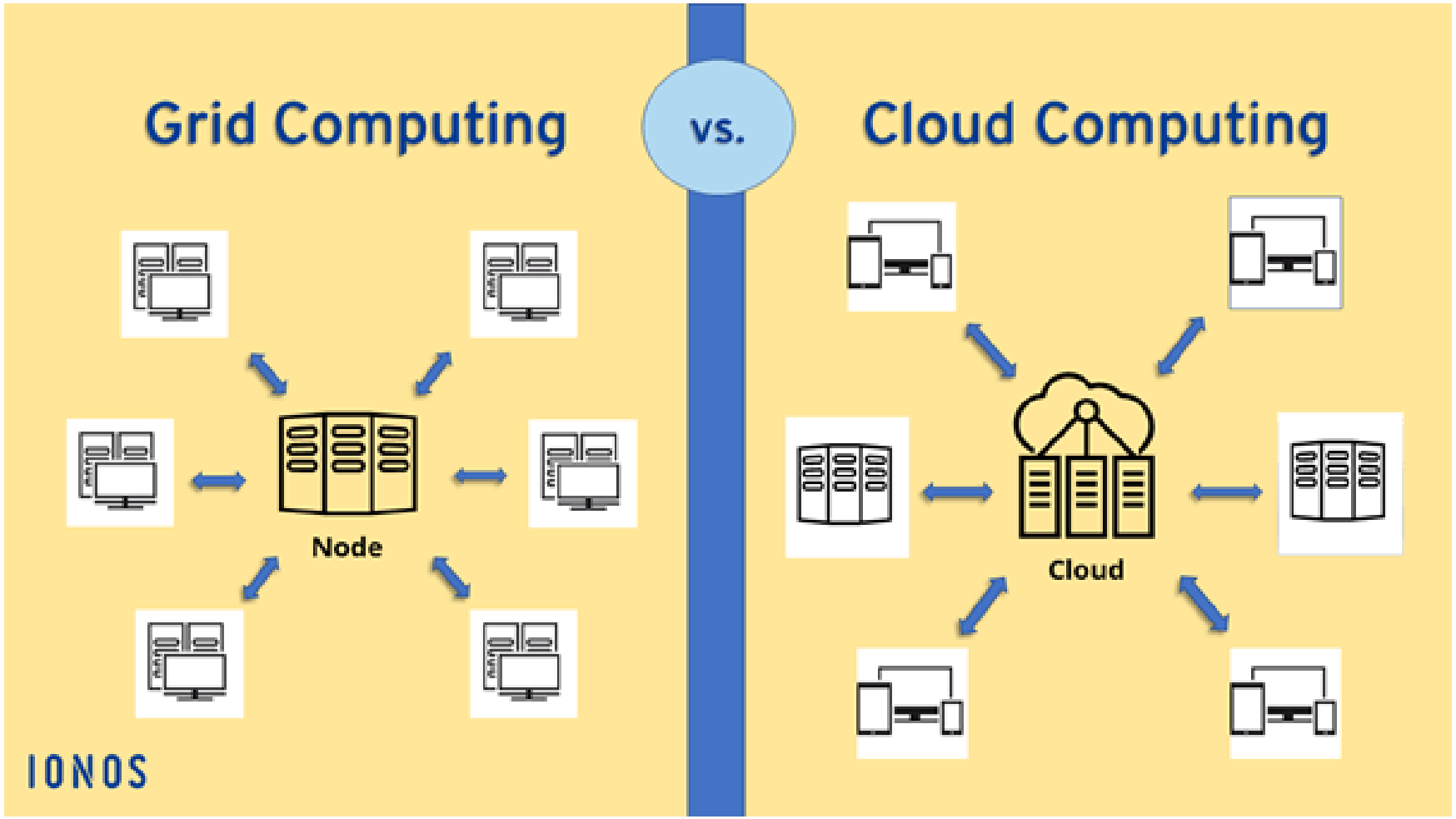
❖ Tính toán lưới (Grid Computing)



4.5 Tính toán lưới (Grid Computing) và ĐTĐM

- Giống:
  - Tăng năng lực tính toán;
  - Tăng khả năng lưu trữ.
- Khác:
  - Mô hình nghiệp vụ;
  - Kiến trúc;
  - Ứng dụng.

4.5 Tính toán lưới (Grid Computing) và ĐTĐM



Tính toán lưới (Grid Computing) và ĐTĐM

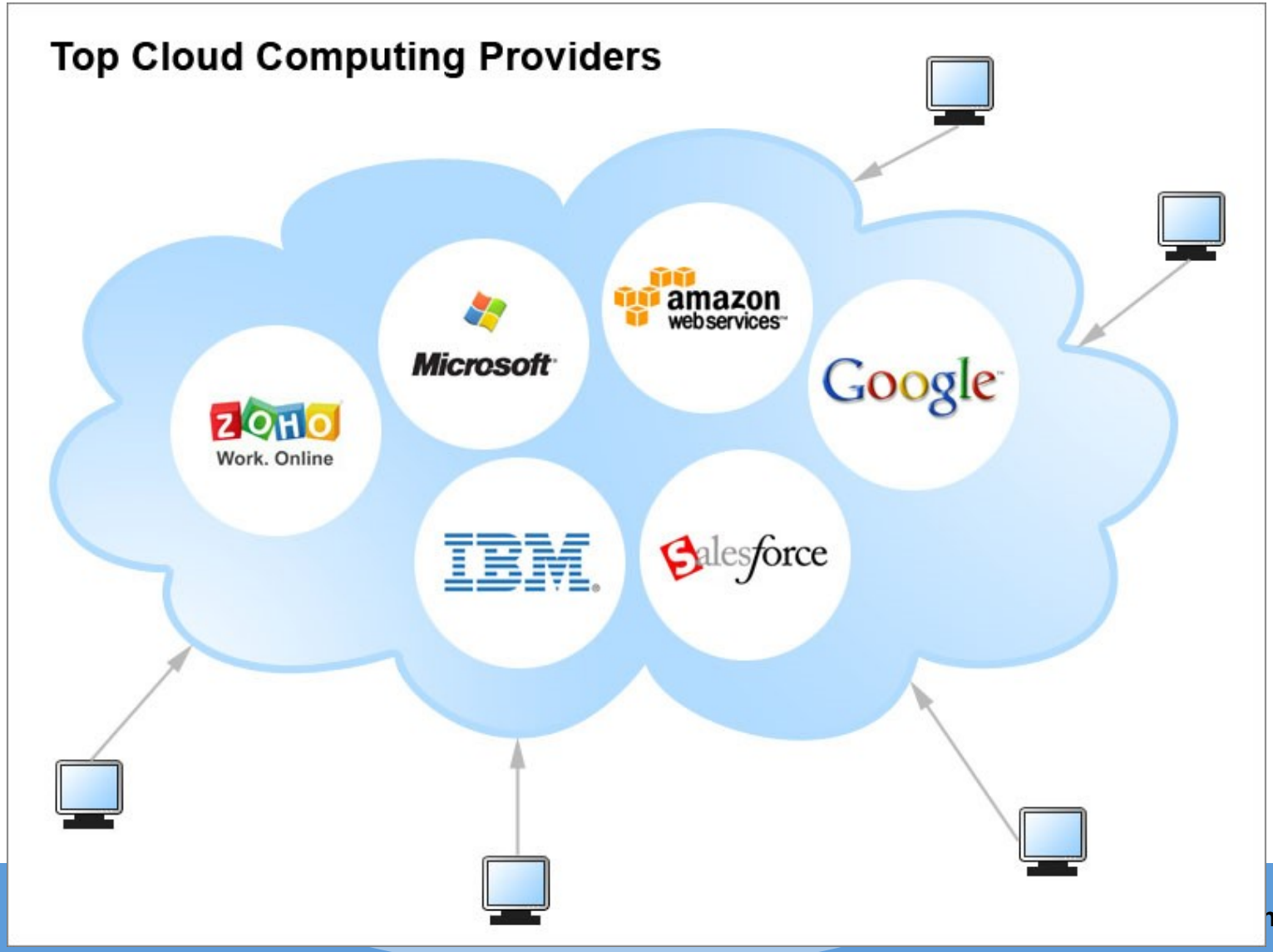
Grid Computing

- Job scheduling is the core value and aim of grid technology, its aim is to use all kinds of resources.
- It can divide a huge task into a lot of independent and no related sub tasks, and then let every node do the jobs.
- Even any node fails and doesn't return result, it doesn't matter; the whole process will not be affected.
- Even one node crashes, the task it should do will be reassigned to other nodes

Cloud Computing

- Computing, cloud computing will make a huge resource pool through grouping all the resources.
- But the resources provided by cloud is to complete a special task.
- For example, a user may apply resource from the resource pool to deploy its application, not submit its task to grid and let grid complete it

4.6 Một số nhà cung cấp dịch vụ và ứng dụng của ĐTĐM



Một số nhà cung cấp dịch vụ ĐTĐM hàng đầu

- Infrastructure-as-a-Service (IaaS)
  - Amazon Web Services
  - Microsoft Azure
- Storage
  - Google Drive
  - Dropbox
  - Box (https://www.box.com)
- Desktop-as-a-Service (DaaS)
  - Citrix
  - VMWare

Một số nhà cung cấp dịch vụ ĐTĐM hàng đầu

- Platform-as-a-Service (PaaS)
  - Google App Engine
  - Red Hat OpenShift
- Software-as-a-Service (SaaS)
  - Salesforce.com (dịch vụ CRM)
  - Insightly (dịch vụ CRM)
  - Gmail
  - Youtube.

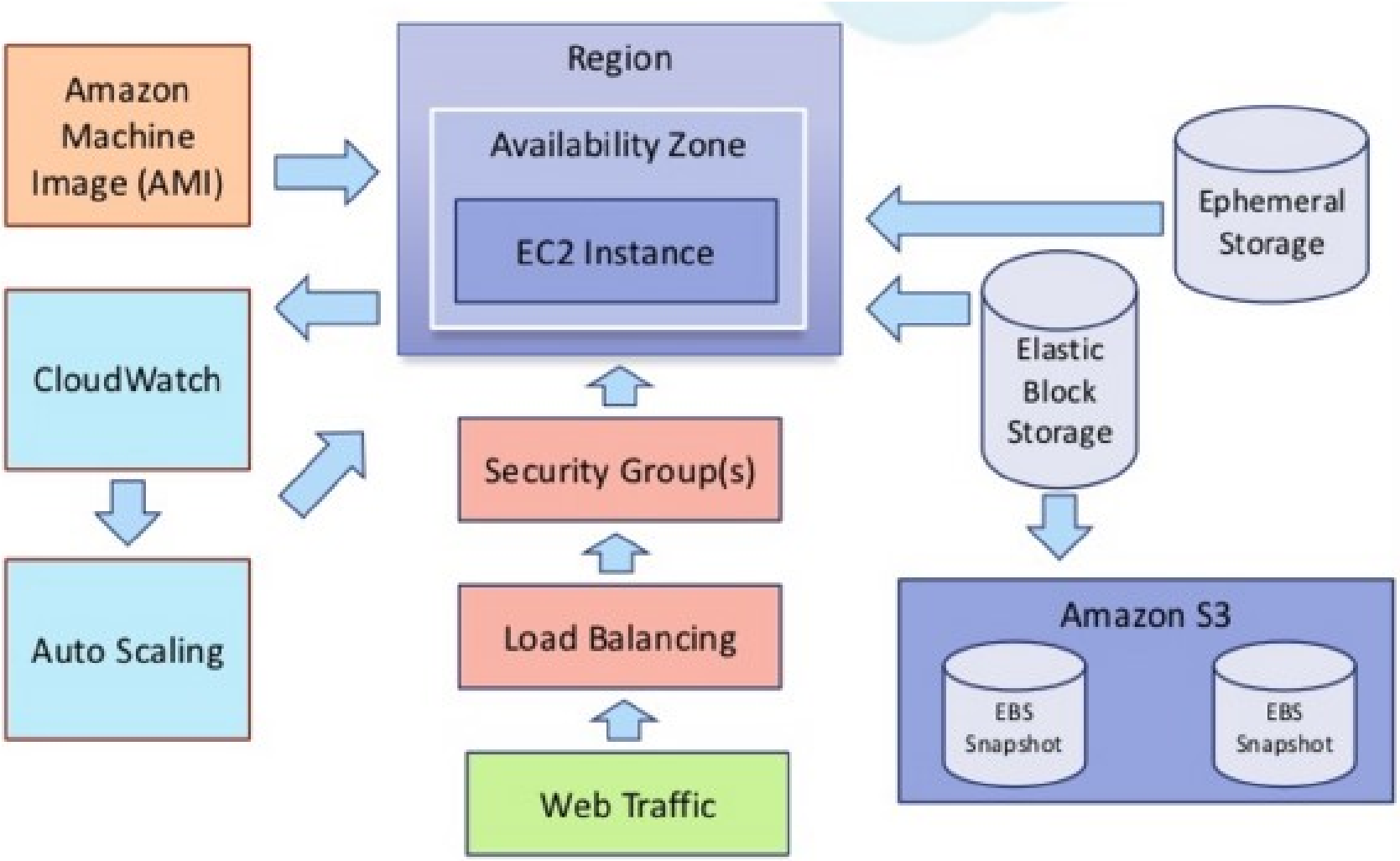
Một số dịch vụ ĐTĐM điển hình

- Amazon EC2
- Google Apps/ Google App Engine

Amazon EC2

- Amazon EC2 là thành trọng yếu của đám mây Amazon;
- Amazon EC2 là dịch vụ kiểu IasS, cung cấp dịch vụ cấp phát, quản lý và thu hồi các máy chủ ảo;
- Khách hàng có thể lựa chọn mua dịch vụ máy chủ ảo với nhiều gói dịch vụ với nền tảng và cấu hình khác nhau:
  - Các máy chủ trên nền tảng Windows/Linux;
  - Cấu hình CPU, RAM, HDD,...

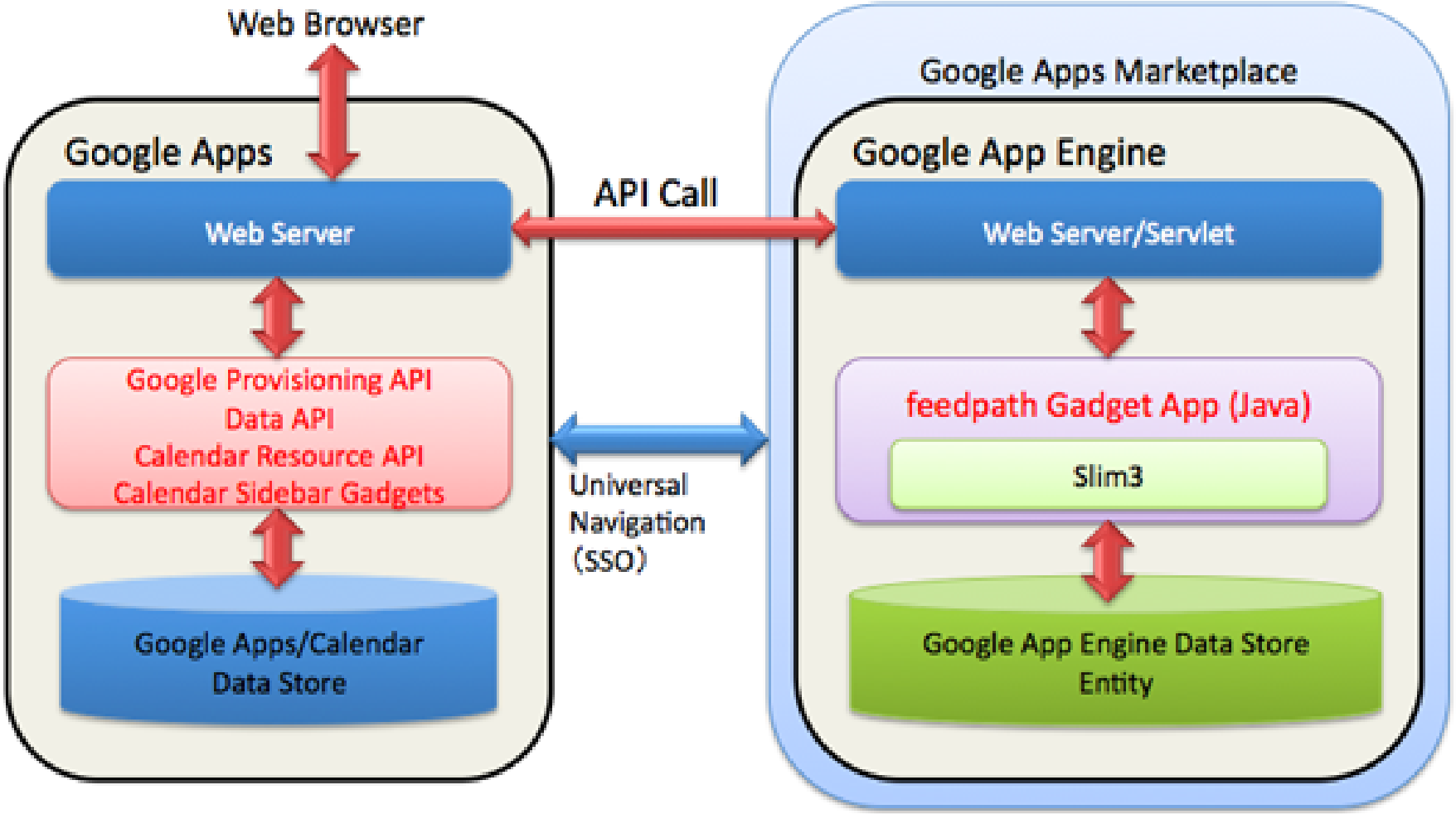
Kiến trúc Amazon EC2



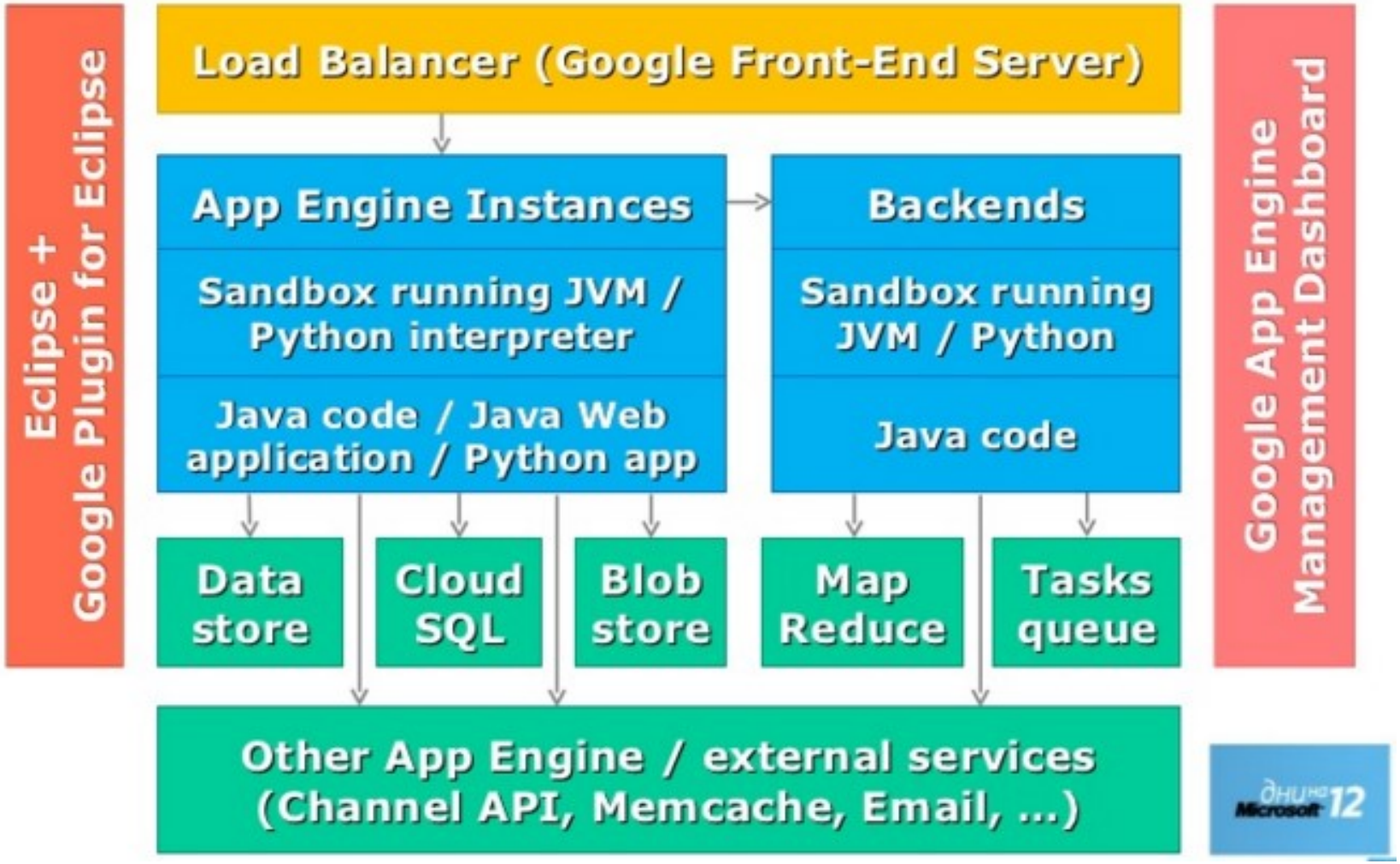
Google App Engine

- Google App Engine là một dịch vụ kiểu PasS, cho phép người dùng phát triển và cài đặt các ứng dụng web trên hệ thống do Google quản lý;
- Các ứng dụng được đặt vào các *sandbox* và có thể chạy trên nhiều máy chủ;
- Hỗ trợ tính năng tự động mở rộng quy mô khi số lượng yêu cầu tăng;
  - Google App Engine sẽ cấp bổ sung tài nguyên khi yêu cầu tăng.
- Hiện hỗ trợ các ngôn ngữ lập trình Java, Python và PHP.

Google App Engine và Google Apps

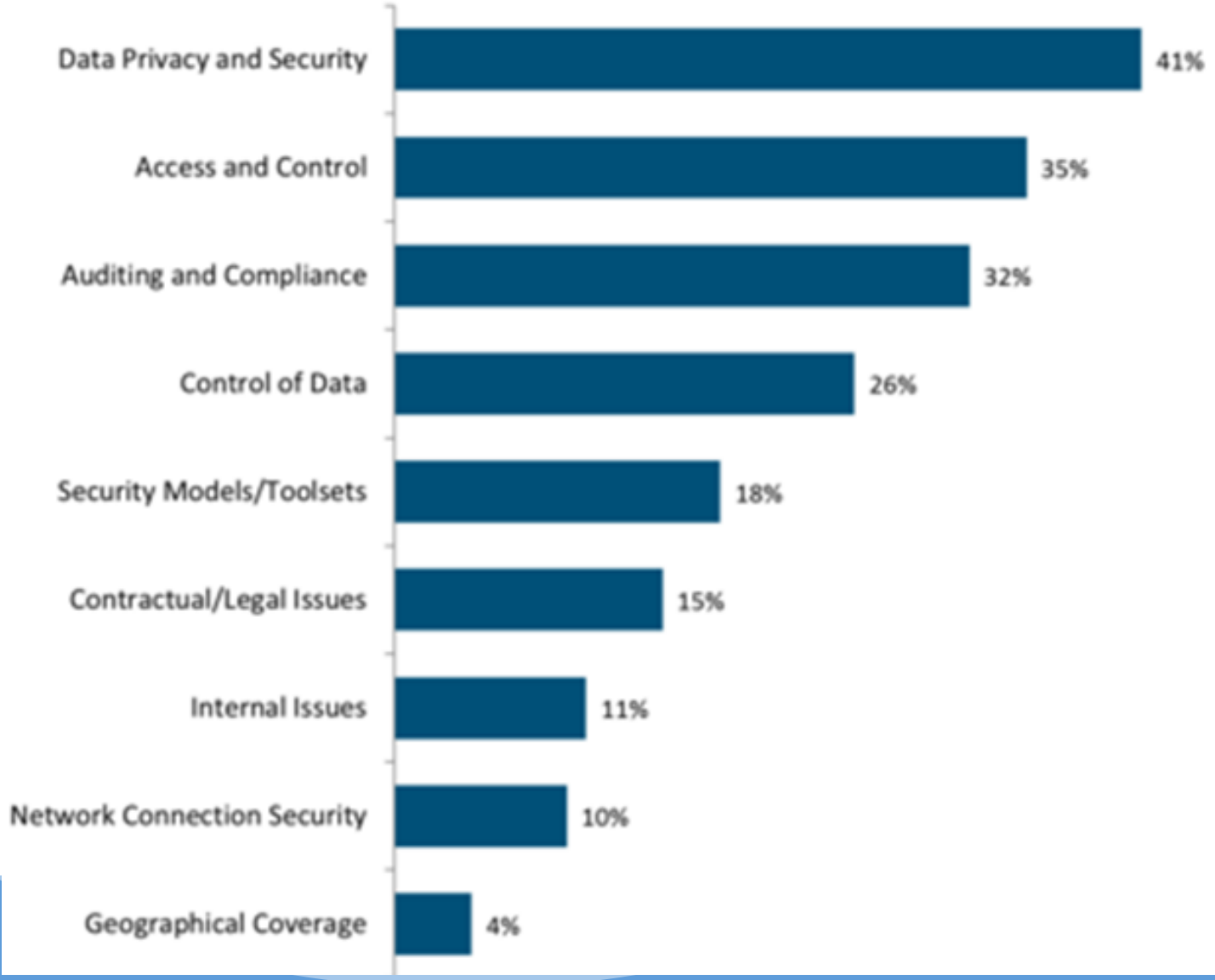


Kiến trúc Google App Engine



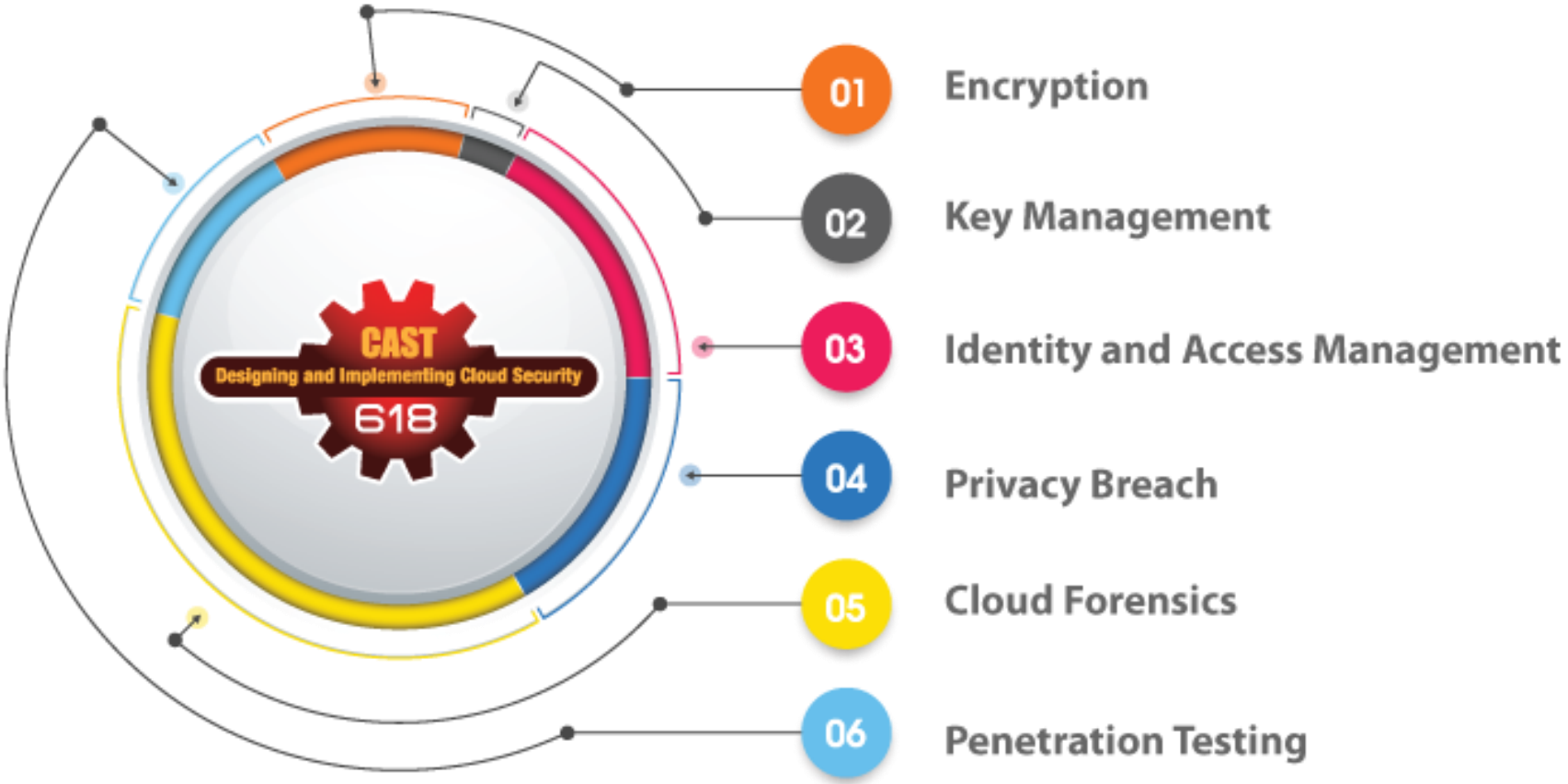
4.7 Các vấn đề bảo mật ĐTĐM

Các vấn đề bảo mật hàng đầu đối với điện toán đám mây



4.7 Các vấn đề bảo mật ĐTĐM

The Program Addresses Critical Cloud Governance, Risk Management, and Compliance (GRC) Issues



4.8 Các biện pháp bảo mật ĐTĐM

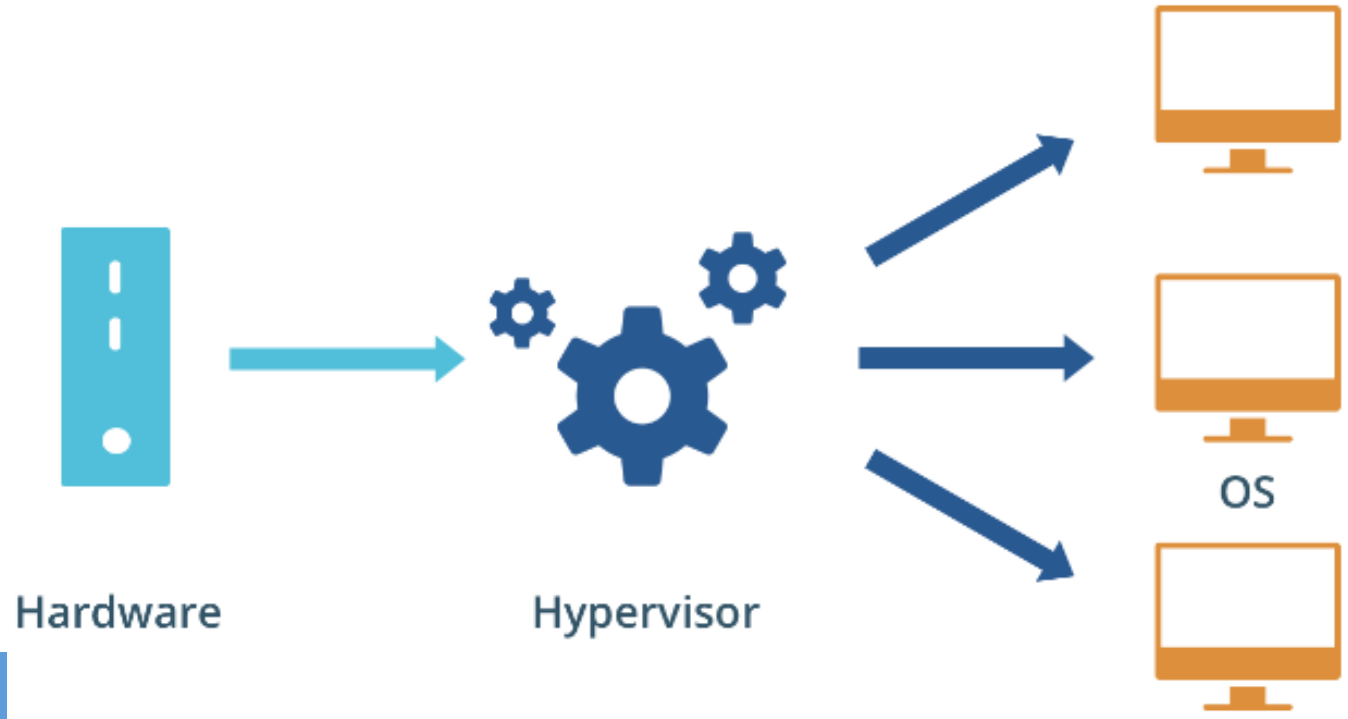
- Bảo mật dữ liệu và ứng dụng
- Bảo mật dữ liệu di chuyển
- Thỏa thuận cấp độ dịch vụ
- Mã hóa dữ liệu
- Bảo mật điểm truy cập web
- Tuân thủ các chuẩn/qui định.

Bảo mật dữ liệu và ứng dụng

- Bảo mật trình quản lý máy ảo
- Bảo mật các host
- Vấn đề các máy khách.

Bảo mật trình quản lý máy ảo

- Trình quản lý máy ảo (Hypervisor hay Virtual machine manager (VMM) là một kỹ thuật ảo hóa phần cứng cho phép nhiều hệ điều hành khách (Guest OS) chạy đồng thời trên 1 máy tính nền.



Bảo mật trình quản lý máy ảo

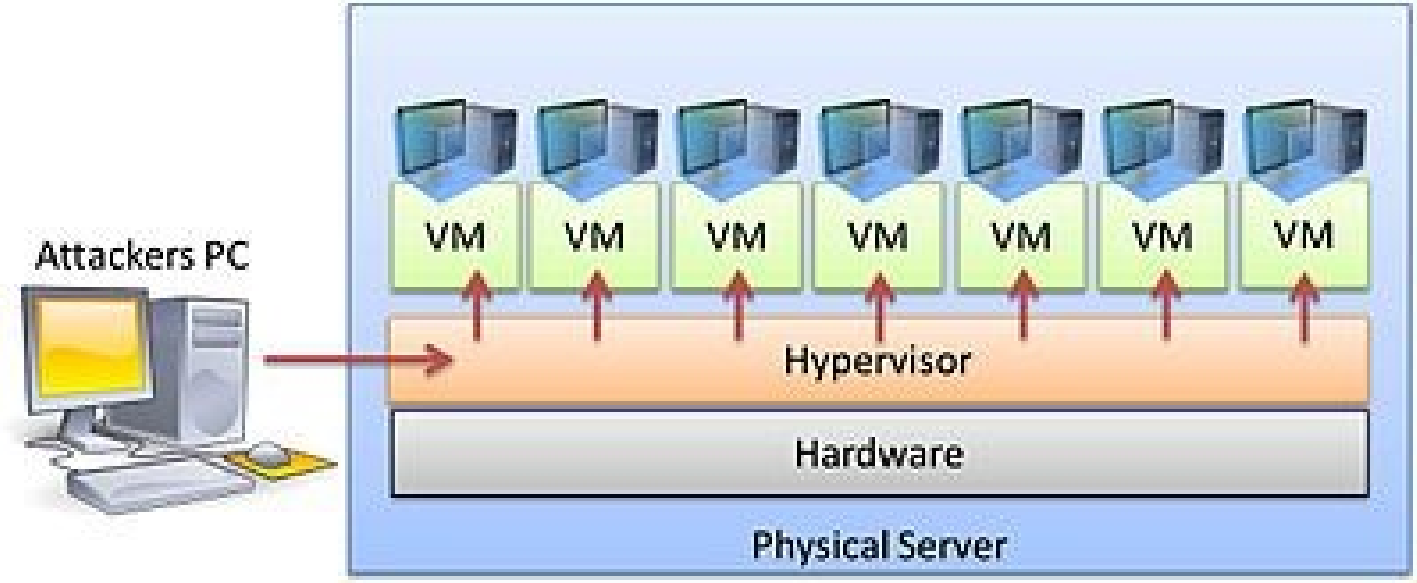
- Ảo hóa là một trong các công nghệ nền tảng của ĐTĐM;
  - Ảo hóa giúp ĐTĐM có khả năng mở rộng và tính linh hoạt trong cung cấp dịch vụ cho người dùng.
- VMM có nhiệm vụ:
  - Tạo các máy ảo và cấp phát các tài nguyên cho các máy ảo;
  - Xóa các máy ảo.
- VMM hoạt động như 1 đường dẫn 2 chiều vào/ra từng máy ảo;
  - Nếu 1 trong 2 thực thể (VMM hoặc máy ảo) bị kiểm soát sẽ gây nguy hiểm cho thực thể còn lại.

Bảo mật trình quản lý máy ảo

- Các VMM được thiết kế hoạt động trong 1 môi trường tách biệt với các máy ảo.
  - VMM chạy trong không gian của hệ điều hành, cùng với các trình điều khiển thiết bị trong không gian nhân HĐH;
  - Các máy ảo chạy trong các hộp cát (sandbox).
- Do đó, một trong những mối lo ngại về bảo mật lớn nhất đối với VMM là việc kẻ xâm nhập thiết lập các kênh bí mật—"hyperjacking".
  - Nếu kẻ xâm nhập thành công trong việc thiết lập kênh bí mật, bằng cách sửa đổi nội dung tệp hoặc thông qua thời gian, thông tin có thể bị rò rỉ từ phiên bản máy ảo này sang phiên bản máy ảo khác.

Bảo mật trình quản lý máy ảo

- Để một cuộc tấn công hyperjacking thành công, kẻ tấn công sẽ phải kiểm soát bộ ảo hóa bằng các phương pháp sau:
  - Đưa một VMM lừa đảo vào bên dưới VMM ban đầu
  - Trực tiếp giành được quyền kiểm soát của VMM ban đầu
  - Chạy một VMM giả mạo trên một VMM hiện có.



Bảo mật trình quản lý máy ảo

- Ngoài ra, VMM là bộ điều khiển của toàn bộ các máy ảo, nó là một điểm lỗi duy nhất (single point of failure) trong bất kỳ kiến trúc điện toán đám mây nào.
  - Nếu kẻ tấn công có thể kiểm soát VMM, hắn ta có thể kiểm soát tất cả các máy ảo do VMM đó quản lý.
    - Kẻ tấn công có thể tạo cung như xóa các máy ảo tùy ý.
    - Kẻ tấn công có thể thực hiện dạng tấn công DoS bằng cách tắt VMM --> dẫn đến tất cả các máy ảo chạy trên VMM đó ngừng hoạt động.

Bảo mật trình quản lý máy ảo

❖ Các biện pháp bảo mật VMM và các máy ảo:

- Kiểm soát truy cập: VMM và các tham số cấu hình của nó chỉ có thể được truy cập bởi người dùng được ủy quyền. Thông qua các hệ thống xác thực và ủy quyền, quyền truy cập phải được hạn chế.
- Cách ly các máy ảo : VMM phải đảm bảo rằng các máy ảo được tách biệt với nhau và hoạt động của chúng không ảnh hưởng đến tính bảo mật hoặc tính ổn định của các máy ảo khác, VMM hoặc cả hai.
- Phát hiện và giảm thiểu mối đe dọa : VMM phải bao gồm các công cụ bảo mật có thể nhanh chóng xác định và giải quyết các mối đe dọa có thể xảy ra. Ví dụ: tường lửa, chương trình chống vi-rút và hệ thống phát hiện xâm nhập.
- Quản lý bản vá : Để giữ an toàn cho bộ ảo hóa và ngăn chặn các lỗ hổng bị khai thác, việc nâng cấp và vá lỗi phần mềm thường xuyên là điều cần thiết.
- Mã hóa dữ liệu : Để ngăn chặn hành vi trộm cắp và truy cập bất hợp pháp, dữ liệu nhạy cảm được lưu trữ trong máy ảo phải được mã hóa.

Bảo mật các host

- Thông qua các host như các máy trạm, người dùng có quyền truy cập vào hệ thống máy ảo và do vậy truy cập vào đám mây. Hai dạng lỗ hổng trong hệ thống có thể bị khai thác gồm:
  - Lỗ hổng thoát sang VMM (Escape-to-hypervisor): cho phép kẻ tấn công xâm nhập vào máy ảo từ một host;
  - Lỗ hổng thoát sang host (Escape-to-host): cho phép lỗ hổng trong máy ảo di chuyển đến các host.

Vấn đề các máy khách

- Các máy khách (Guest machines):
  - Máy khách (máy ảo) chạy hệ điều hành khách cũng có thể gây ra vấn đề bảo mật cho đám mây.
  - Tuy nhiên, các lỗ hổng trong máy ảo khách chỉ giới hạn ở máy đó và chúng hiếm khi ảnh hưởng đến các máy khác trong hệ thống.

Bảo mật dữ liệu di chuyển

- Với dữ liệu di chuyển các biện pháp bảo mật cần được thực hiện gồm:
  - Sử dụng mã hóa đủ mạnh để bảo vệ dữ liệu khách hàng;
  - Tăng cường an toàn truy cập và sử dụng các ứng dụng đám mây;
  - Quản lý đám mây an toàn.

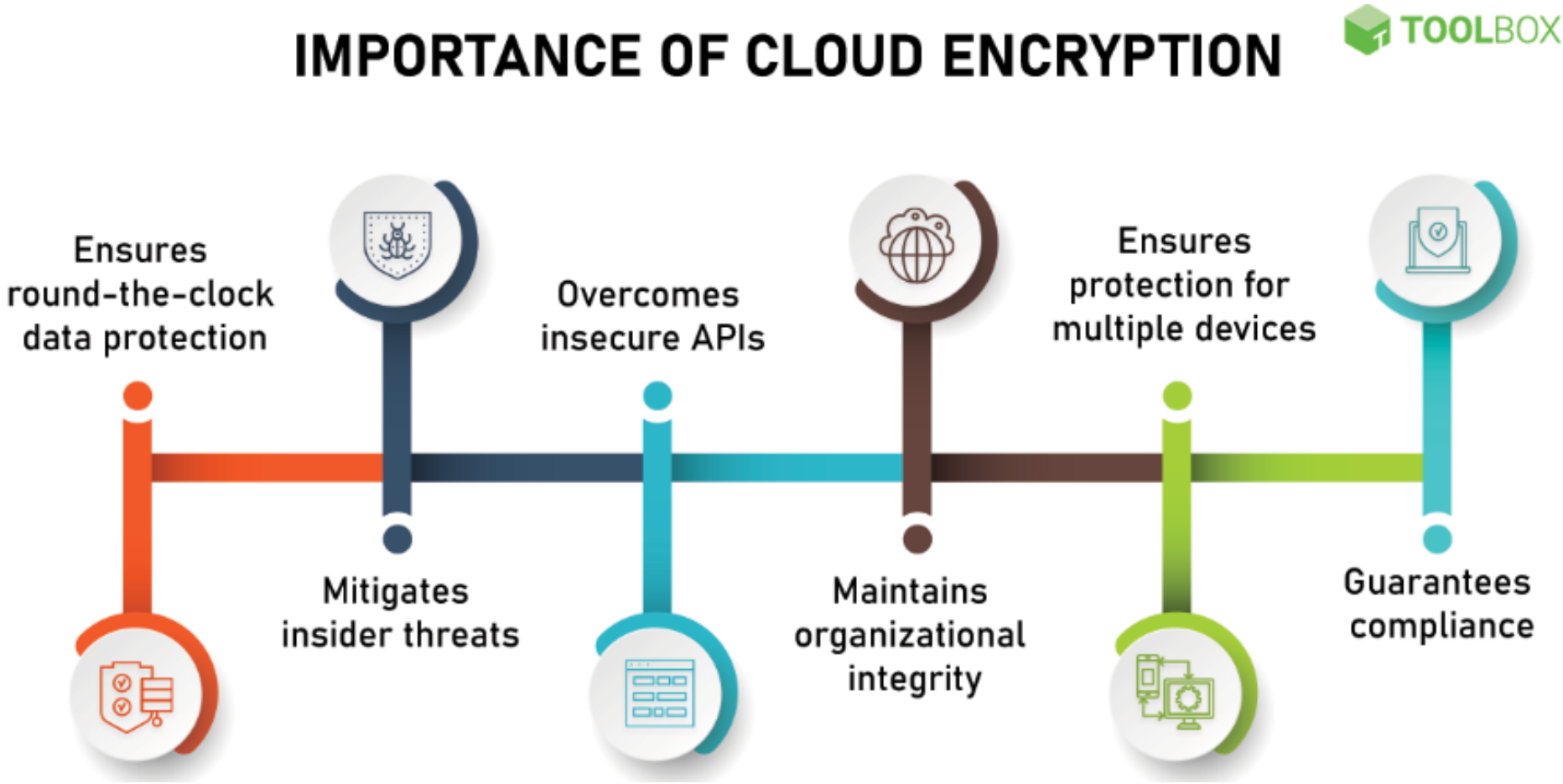
Thỏa thuận cấp độ dịch vụ

- Thỏa thuận cấp độ dịch vụ (Service-level agreement - SLA) là hợp đồng dịch vụ giữa nhà cung cấp dịch vụ và khách hàng xác định mức độ dịch vụ mong đợi về mặt bảo mật, tính khả dụng và hiệu suất.
  - SLA là một loạt hợp đồng dịch vụ giữa nhà cung cấp đám mây và khách hàng để xác định cấp độ dịch vụ dựa trên loại dịch vụ mà khách hàng tìm kiếm vì hiệu quả của các hợp đồng này phụ thuộc vào mức độ tối đa hóa và các dịch vụ này được điều chỉnh phù hợp với nhu cầu cụ thể của từng khách hàng.
  - Ví dụ: tính bảo mật của các dịch vụ mà khách hàng tìm kiếm có thể phụ thuộc vào cấp độ dịch vụ đám mây mà khách hàng đang sử dụng. Để xem những tài liệu này có thể liên quan và phức tạp đến mức nào, hãy lấy một ví dụ về những lo ngại về bảo mật.
    - Đối với IaaS, trách nhiệm bảo mật được chia sẻ với nhà cung cấp chịu trách nhiệm về bảo mật vật lý, môi trường và ảo hóa, trong khi khách hàng đảm nhiệm việc bảo mật trong các ứng dụng, hệ điều hành và những thứ khác.
    - Bây giờ, nếu chúng ta thay đổi mô hình dịch vụ sang SaaS, nhà cung cấp sẽ chịu trách nhiệm về hầu hết mọi khía cạnh bảo mật.

Mã hóa dữ liệu

- Khi dữ liệu rời khỏi điểm truy cập web-cloud điểm cuối ở vị trí của bạn, dữ liệu sẽ di chuyển qua mạng công cộng và được lưu trữ trong môi trường chia sẻ là đám mây.
- Trong môi trường công cộng hoặc chia sẻ, dữ liệu có thể bị chặn và xâm nhập bởi những kẻ xâm nhập từ bên trong và bên ngoài đám mây cũng như bị tấn công thám mã trong quá trình truyền.
- Để ngăn chặn những loại vi phạm này, cần có chế độ xác thực và mã hóa mạnh mẽ.
  - Mã hóa để bảo vệ chống lại mọi loại vi phạm dữ liệu yêu cầu quy trình xác thực và kiểm soát quyền truy cập mạnh mẽ vào tất cả các giao diện tài nguyên đám mây dựa trên web;
  - Mã hóa tất cả truy cập quản trị vào trình ảo hóa đám mây, cũng như tất cả truy cập vào ứng dụng và dữ liệu.

Mã hóa dữ liệu



Mã hóa dữ liệu

Bảo mật điểm truy cập web

- Hầu hết các truy cập đám mây đều dựa trên web.
- Hầu hết các vi phạm bảo mật đối với dữ liệu được lưu trữ đều bắt nguồn từ các ứng dụng web.
- Do đó, cần có các biện pháp kiểm soát bảo mật mạnh mẽ trong API đám mây.

Tuân thủ các chuẩn/qui định

- Do hầu hết các đám mây đều là đám mây công cộng, cộng đồng hoặc đám mây lai và khách hàng sử dụng những đám mây này thường là các doanh nghiệp xử lý dữ liệu cá nhân nên các nhà cung cấp đám mây phải tuân thủ một số quy định của chính quyền, bao gồm:
  - FISMA, HIPAA, SOX và SAS 70 II dành cho đám mây dựa trên ở Hoa Kỳ và
  - Chỉ thị bảo vệ dữ liệu dành cho các đám mây có trụ sở tại EU;
  - Ngoài ra, các nhà cung cấp chấp nhận thanh toán bằng tín dụngthẻ phải tuân thủ PCI DSS.

Tuân thủ các chuẩn/qui định

- FISMA: Federal Information Security Management Act of 2002
- HIPAA : Health Insurance Portability and Accountability Act of 1996
- SOX : Sarbanes-Oxley (SOX) audit
- SAS 70 II : Statement on Auditing Standards No. 70
- PCI DSS : The Payment Card Industry Data Security Standard.