Cloud adoption for project managers with cyber security strategy

Presented By: Hasan T. Emdad | CEO | Kloud Technologies Ltd.
Date: 7-May-2021

- Cloud Computing: Basic Principles
- Showcasing Cloud Data Center
- Cyber Fear & Common Questions
- Use Case Analysis: Securing Data at Rest Stored in a Cloud Infra
- Fear vs Reality

Presentation

Approach

Cloud Computing: Basic Principles

Defining Cloud Computing

- Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet.- Wikipedia
- The expression *cloud* is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not inspected further in a given context.

- The term *cloud* has been used to refer to platforms for **distributed computing**
- Virtualization and resource scaling is ‘heart’ of Cloud

Definition from NIST

Cloud computing is a compilation of **existing techniques and technologies**, packaged within a **new infrastructure paradigm** that offers **improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources**.

What cloud gives us, generally

low initial capital investment

shorter start-up time for new services

lower maintenance and operation costs

higher utilization through virtualization

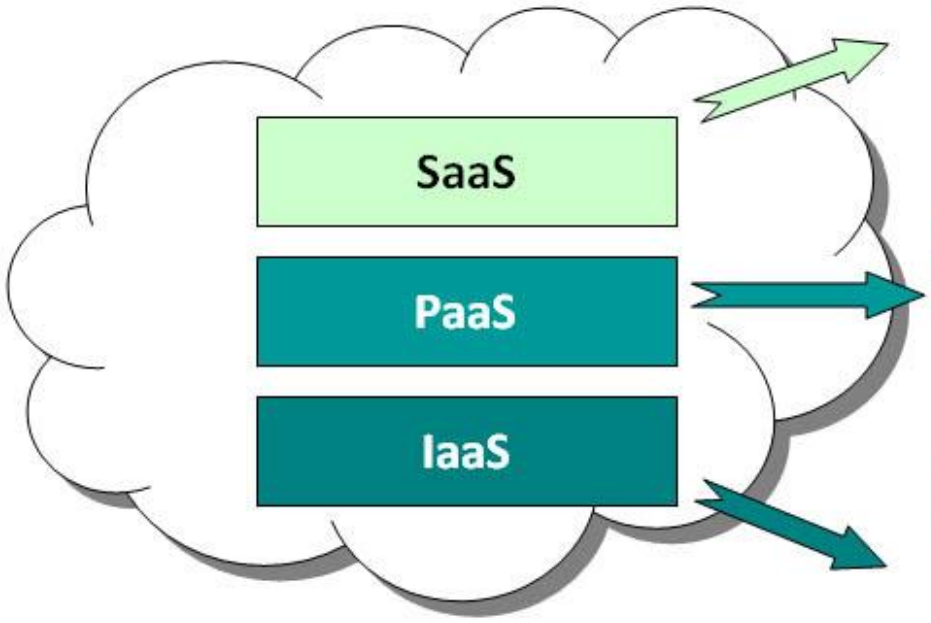
easier disaster recovery

Cloud Computing Background

- Features
  - Use of internet-based services to support business process
  - Rent IT-services on a utility-like basis
- Attributes
  - Rapid deployment
  - Low startup costs/ capital investments
  - Costs based on usage or subscription
  - Multi-tenant sharing of services/ resources
- Essential characteristics
  - On demand self-service
  - Ubiquitous network access
  - Location independent resource pooling
  - Rapid elasticity
  - Measured service

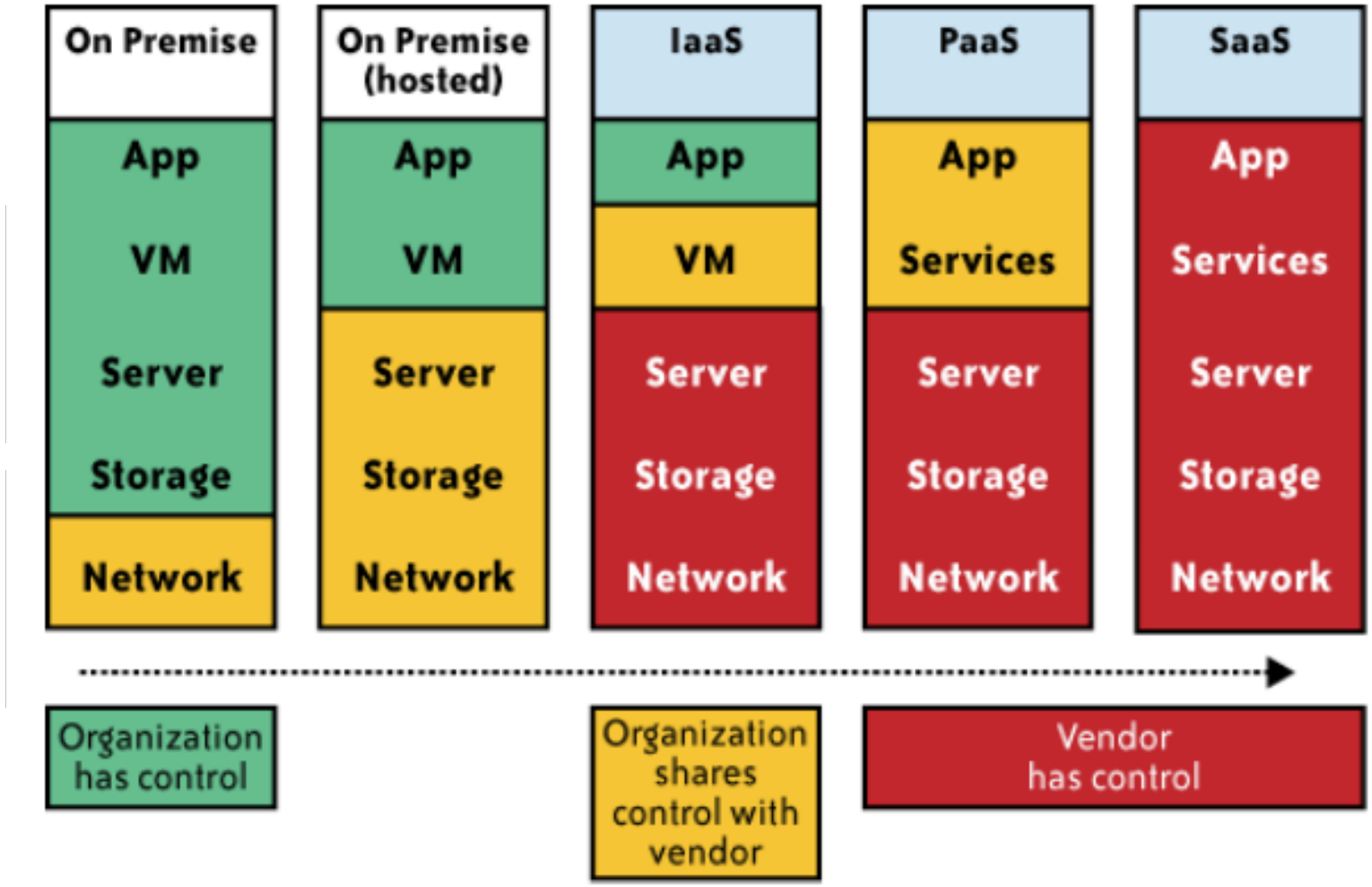
From: NIST

Service Model

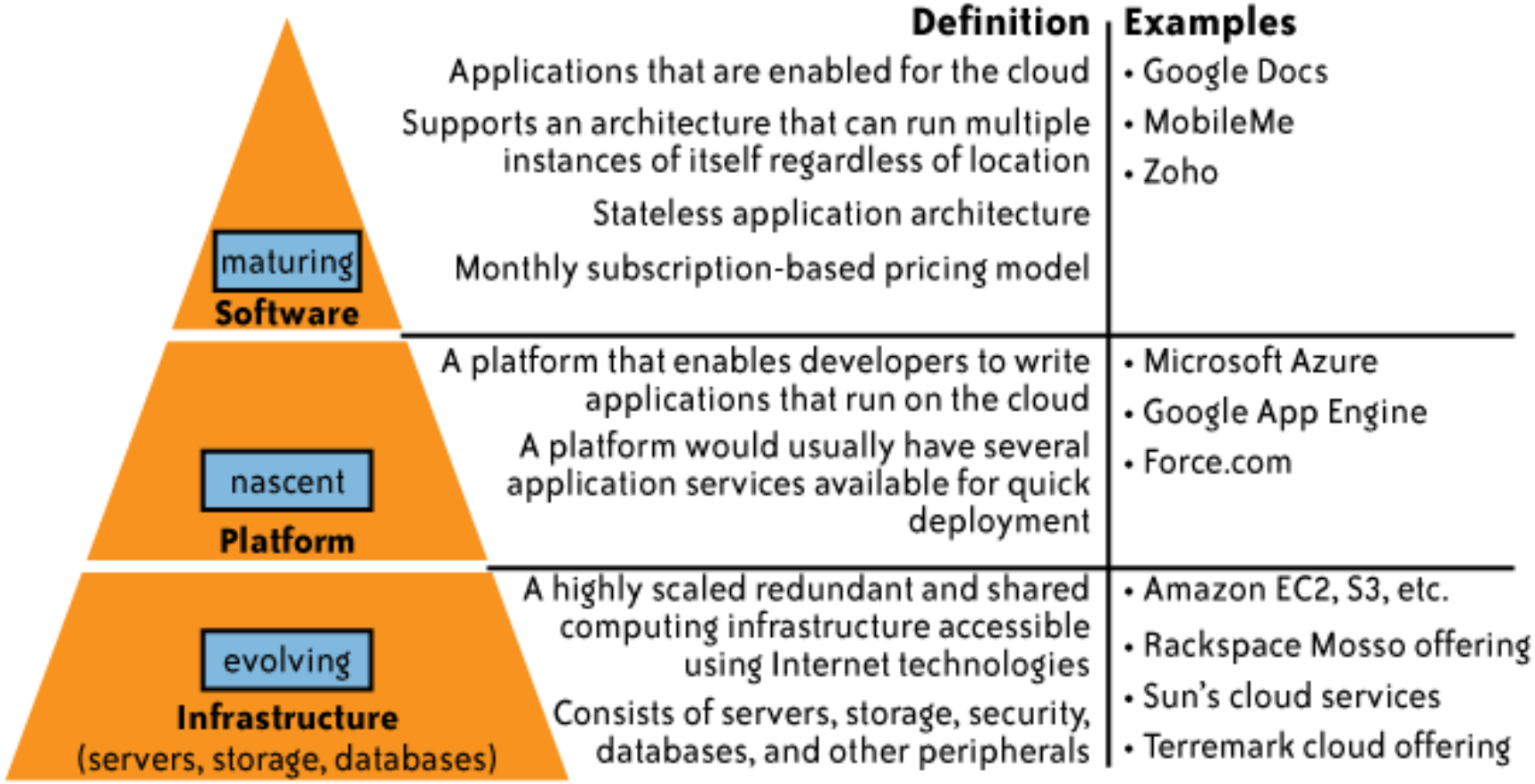


Who Uses It	What Services are available	Why use it?
Business Users	EMail, Office Automation, CRM, Website Testing, Wiki, Blog, Virtual Desktop ...	To complete business tasks
Developers and Deployers	Service and application test, development, integration and deployment	Create or deploy applications and services for users
System Managers	Virtual machines, operating systems, message queues, networks, storage, CPU, memory, backup services	Create platforms for service and application test, development, integration and deployment

Impact of cloud computing on the governance structure of IT organizations



Delivery Models



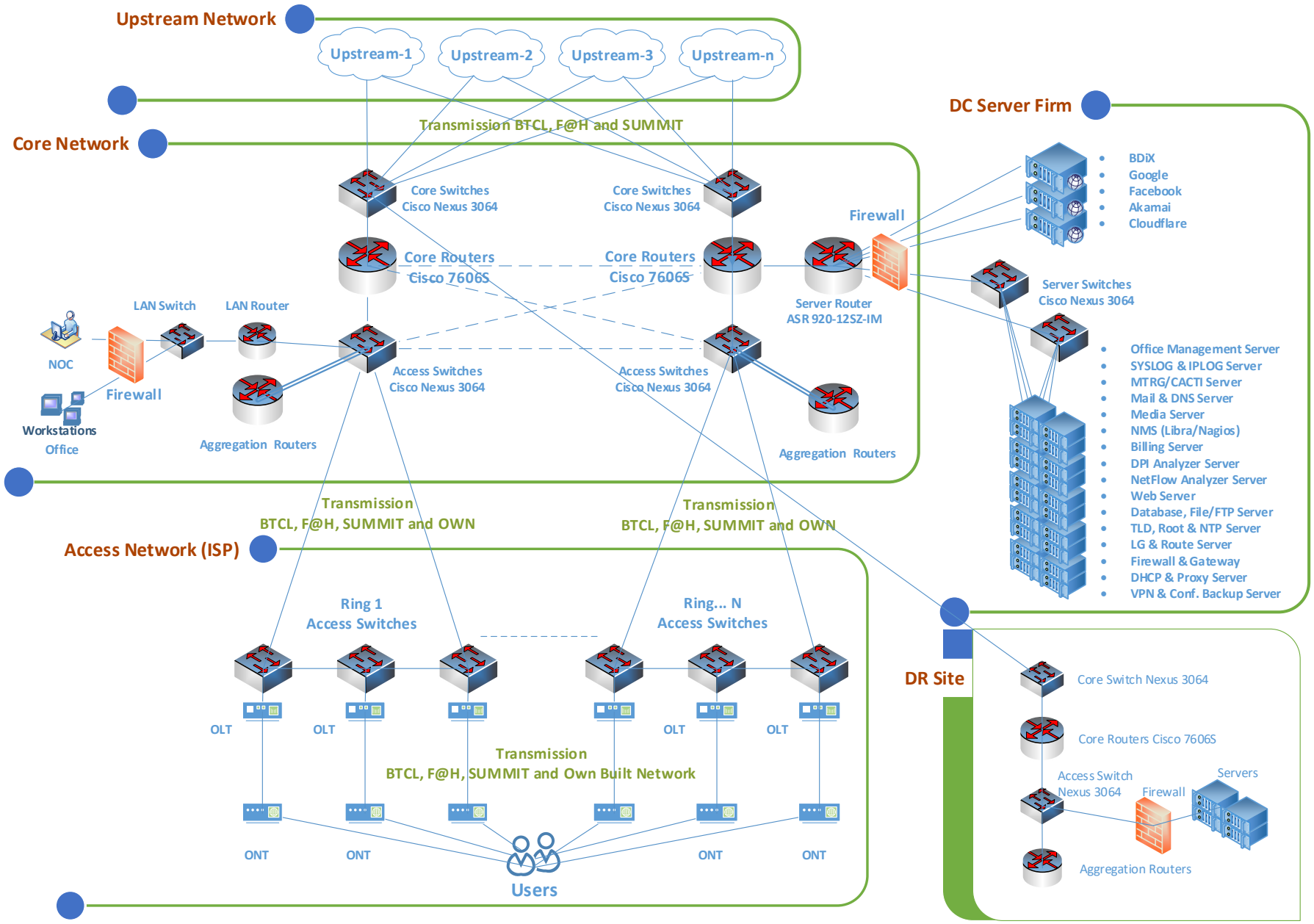
While cloud-based software services are maturing,
Cloud platform and infrastructure offering are still in their early stages !

Src: Cloud Security and Privacy by Mather and Kumaraswamy

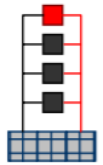
Typical Fear Factor of Cloud Adoption

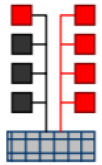
- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Showcasing Cloud Data Center


Upstream Network
Upstream-1
Upstream-2
Upstream-3
Upstream-n
Transmission BTCL, F@H and SUMMIT
Core Network
Core Switches
Cisco Nexus 3064
Core Switches
Cisco Nexus 3064
Firewall
Core Routers
Cisco 7606S
Core Routers
Cisco 7606S
Server Router
ASR 920-12SZ-IM
LAN Switch
LAN Router
NOC
Firewall
Workstations
Office
Access Switches
Cisco Nexus 3064
Access Switches
Cisco Nexus 3064
Aggregation Routers
Aggregation Routers
DC Server Firm
BDiX
Google
Facebook
Akamai
Cloudflare
Server Switches
Cisco Nexus 3064
Office Management Server
SYSLOG & IPLOG Server
MTRG/CACTI Server
Mail & DNS Server
Media Server
NMS (Libra/Nagios)
Billing Server
DPI Analyzer Server
NetFlow Analyzer Server
Web Server
Database, File/FTP Server
TLD, Root & NTP Server
LG & Route Server
Firewall & Gateway
DHCP & Proxy Server
VPN & Conf. Backup Server
Transmission
BTCL, F@H, SUMMIT and OWN
Transmission
BTCL, F@H, SUMMIT and OWN
Access Network (ISP)
Ring 1
Access Switches
Ring... N
Access Switches
OLT
OLT
OLT
OLT
OLT
Transmission
BTCL, F@H, SUMMIT and Own Built Network
ONT
ONT
ONT
ONT
Users
DR Site
Core Switch Nexus 3064
Core Routers Cisco 7606S
Access Switch
Nexus 3064
Firewall
Servers
Aggregation Routers

PDC Tier





Tier	I	II	III	IV
Components	Need only (N)	N + 1	N + 1	2 (N + 1)
Delivery Paths	One only	One only	One active One passive	Two active
Single Points of Failure	Yes	Yes	Yes	No
Concurrently Maintainable	No	Components only	Yes	Yes
Projected Availability / Downtime per Year	99.671% 28.8 hours	99.749% 22.0 hours	99.982% 1.6 hours	99.995% 0.4 hours
Tier	I	II	III	IV

Tiering system courtesy of
The Uptime Institute

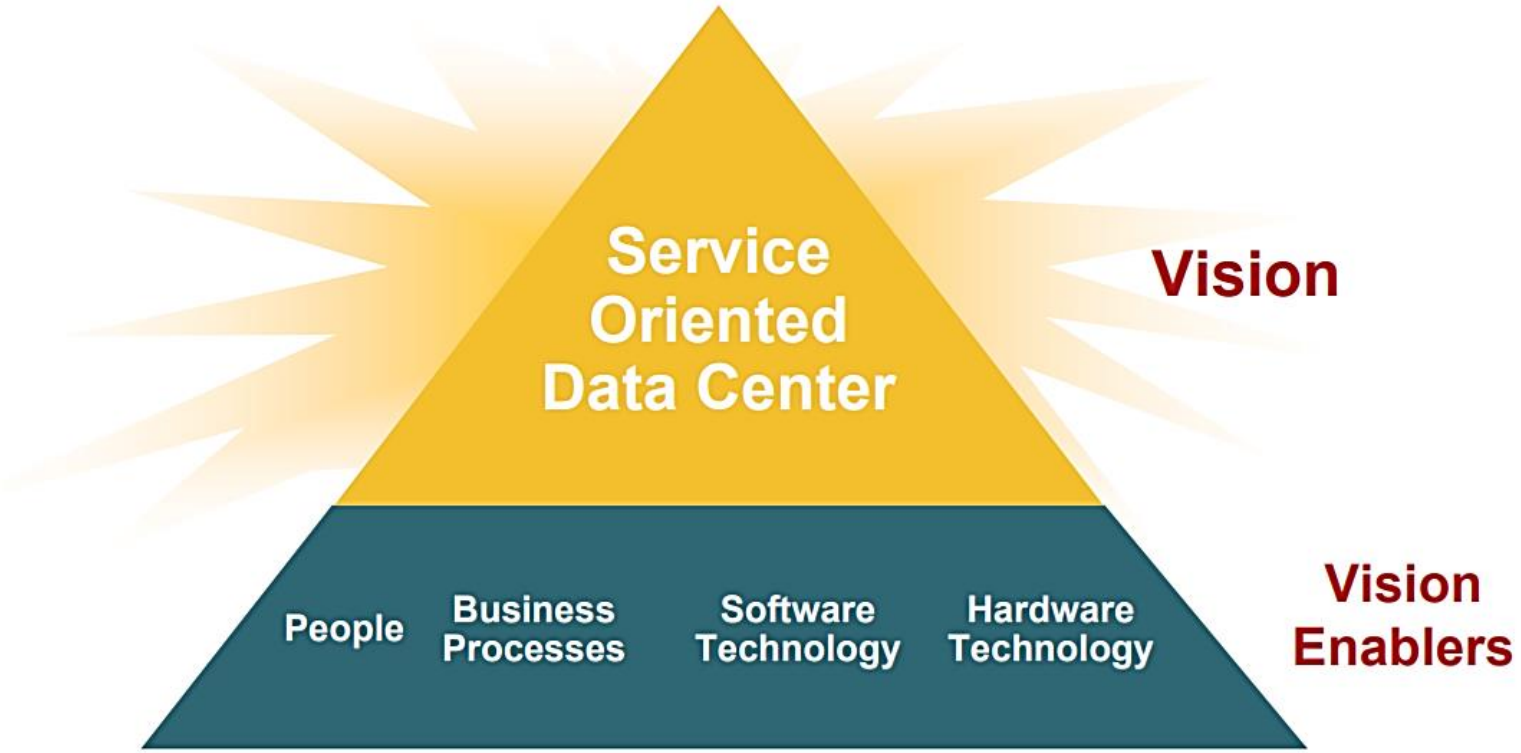
Existing DDCs

Existing PDCs

New PDC

Software Oriented Data Center

- Pooled Virtual Resources
- Automatic Service Provisioning
- Standard Services Based for IaaS, PaaS & SaaS
- Bundled with Enterprise PKI for secure Infrastructure
- Intelligent Unified DC Network
- Hyper Converged Infrastructure



Providers treating its customers

- **The core issue here is the levels of trust**
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

Cyber Fear & Common Questions

Security and Privacy Issues in Cloud Computing

Infrastructure Security- Network, Host & Application

Data Security and Storage- Data in transit, Data at rest, Data Processing

Identity and Access Management (IAM)- Authentication, SSO, m-Factor

Privacy

Taxonomy of Fear

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

From: www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user's own data centers

From: www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

From: www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

From: www.cs.jhu.edu/~ragib/sp10/cs412

Cyber Threat Model

A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

From www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Outside attacker

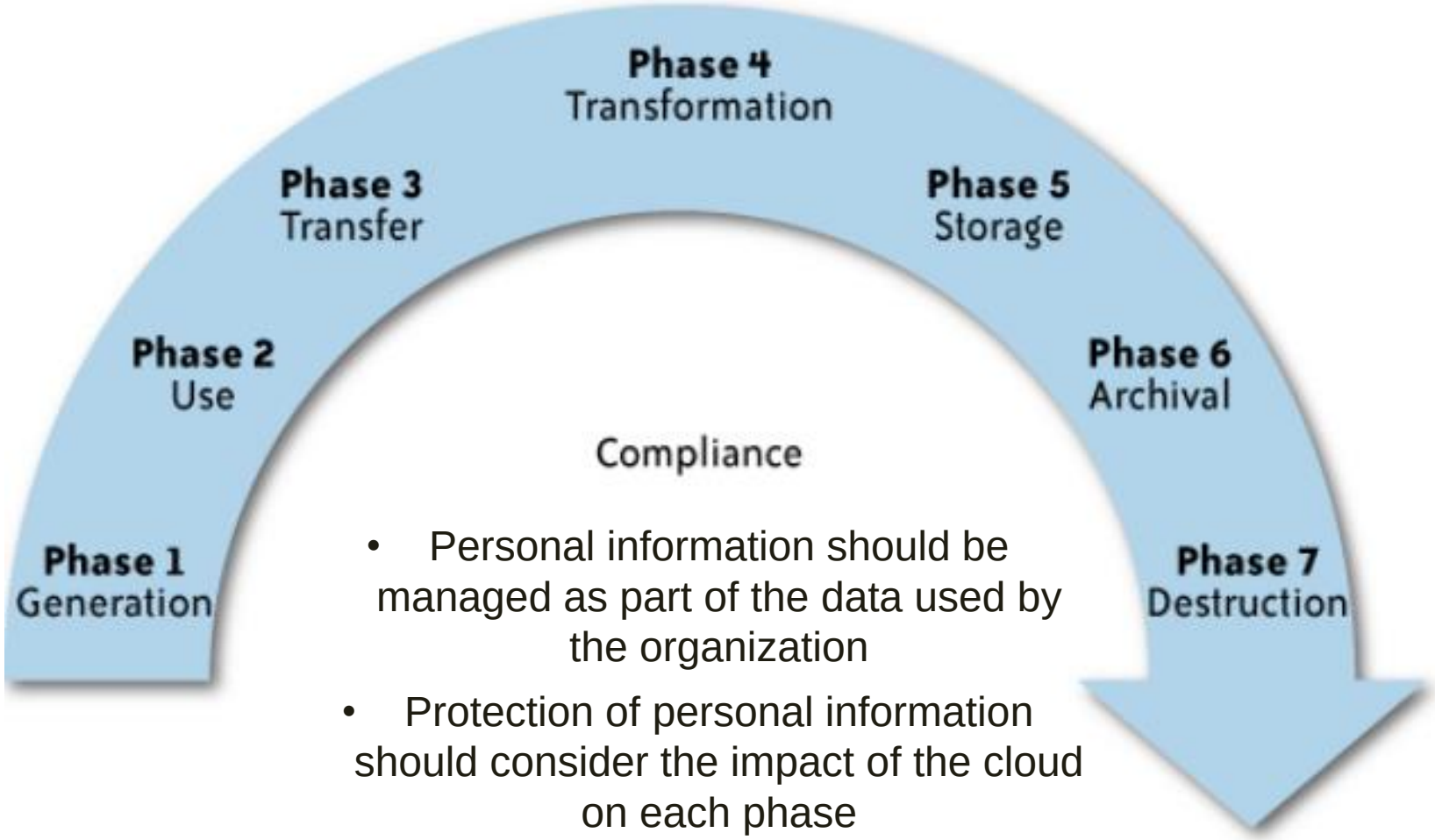
- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

What is the data life cycle Key Privacy Concerns from Managerial Perspective?



- Personal information should be managed as part of the data used by the organization
- Protection of personal information should consider the impact of the cloud on each phase

From: Cloud Security and Privacy by Mather and Kumaraswamy

Auditing, monitoring and risk management

- How can organizations monitor their Content Security Policy-CSP
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.
  - These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

Possible Solutions

- Minimize Lack of Trust
  - Policy Language
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management
  - Identity Management (IDM)
- Minimize Multi-tenancy

Use Case Analysis: Securing Data at Rest Stored in a Cloud Infra

What did they do?

- Simple technique implemented with Open Source software solves the confidentiality of data stored on Cloud Computing Infrastructure by using public key encryption to render stored data at rest unreadable by unauthorized personnel, including system administrators of the cloud computing service on which the data is stored
- Used it on a service where confidentiality is critical – a scanning application that validates external firewall implementations

Problem Scope

- Goal is to ensure the confidentiality of data at rest
- “Data at rest” means that the data that is stored in a readable form on a Cloud Computing service, whether in a storage product like AWS S3 or in a virtual machine

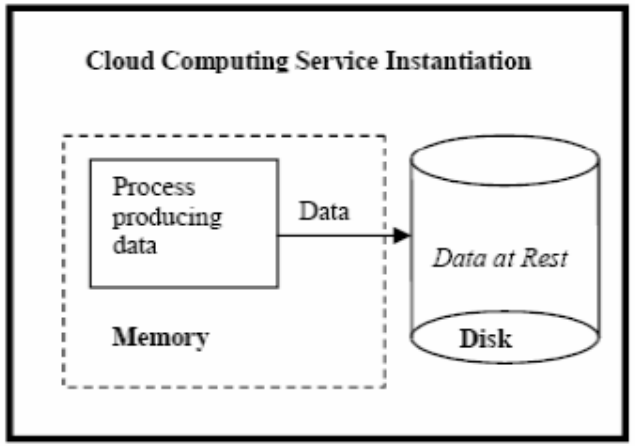


Fig. 1. Process in a Cloud Computing Infrastructure producing Data at Rest

Problem Scope (cont.)

- To protect data at rest, they want to prevent other users in the cloud infrastructure who might have access to the same storage from reading the data our process has stored
- They also want to prevent system administrators who run the cloud computing service from reading the data.
- They assume that it is unlikely for an adversary to snoop on the contents of memory.
  - If the adversary had that capability, it is unlikely that we could trust the confidentiality of any of the data that we generated there.

Problem Scope (cont.)

- While the administrative staff of the cloud computing service could theoretically monitor the data moving in memory before it is stored in disk, we believe that administrative and legal controls should prevent this from happening.
- They also do not guard against the modification of the data at rest, although we are likely to be able to detect this.

Solution Design

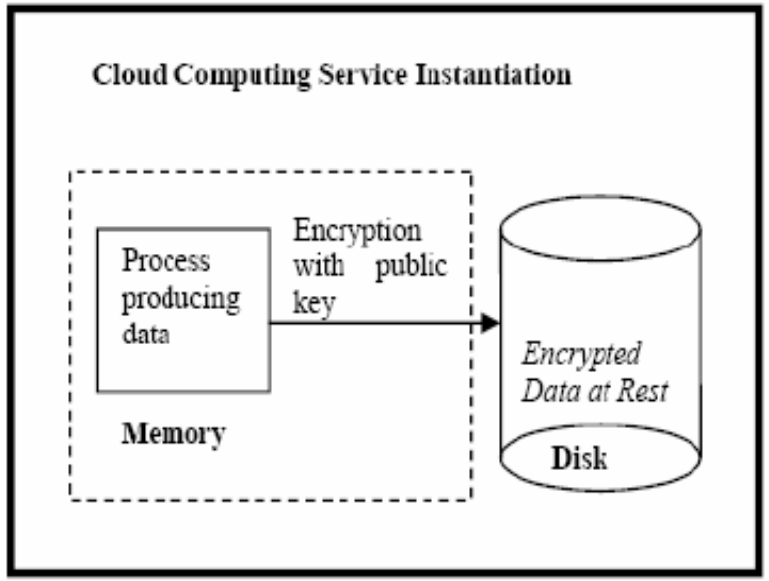


Fig. 2. Process in a Cloud Computing Infrastructure producing Encrypted Data at Rest

Solution Design (cont.)

- On a trusted host, collect the encrypted data, as shown in Figure 3, and decrypt it with the collection agent's private key which stays on that host. Note that in this case, we are in exclusive control of the private key, which the cloud service provider has no view or control over.
- They will discuss this feature of our solution later.

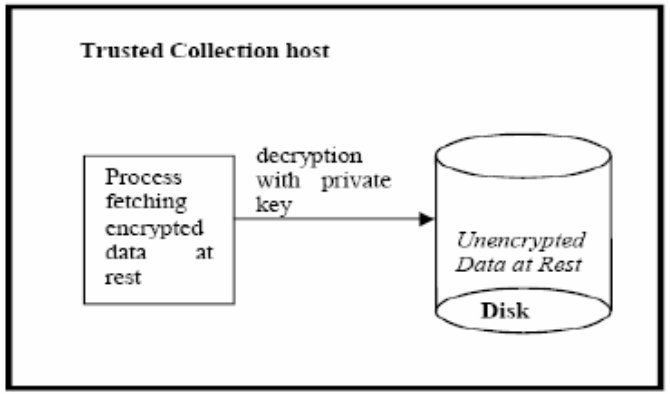


Fig. 3. Process in a Cloud Computing Infrastructure producing Encrypted Data at Rest

More Example Services coupled with security

- Microsoft Office Signing
- PDF Document Signing
- Email Signing and Encryption
- Code Signing
- VPN (IPSec) encryption
- TLS (Microsoft Exchange , Lotus or Mail Server Signing)
- Custom Web Form Signing
- 2 FA authentication and Signing
- Secure Virtual Desktop Login

Fear vs Reality

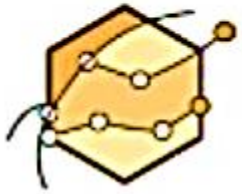
6 Advantages & Benefits as seen by AWS

Trade capital expense for variable expense.

Increase speed and agility.

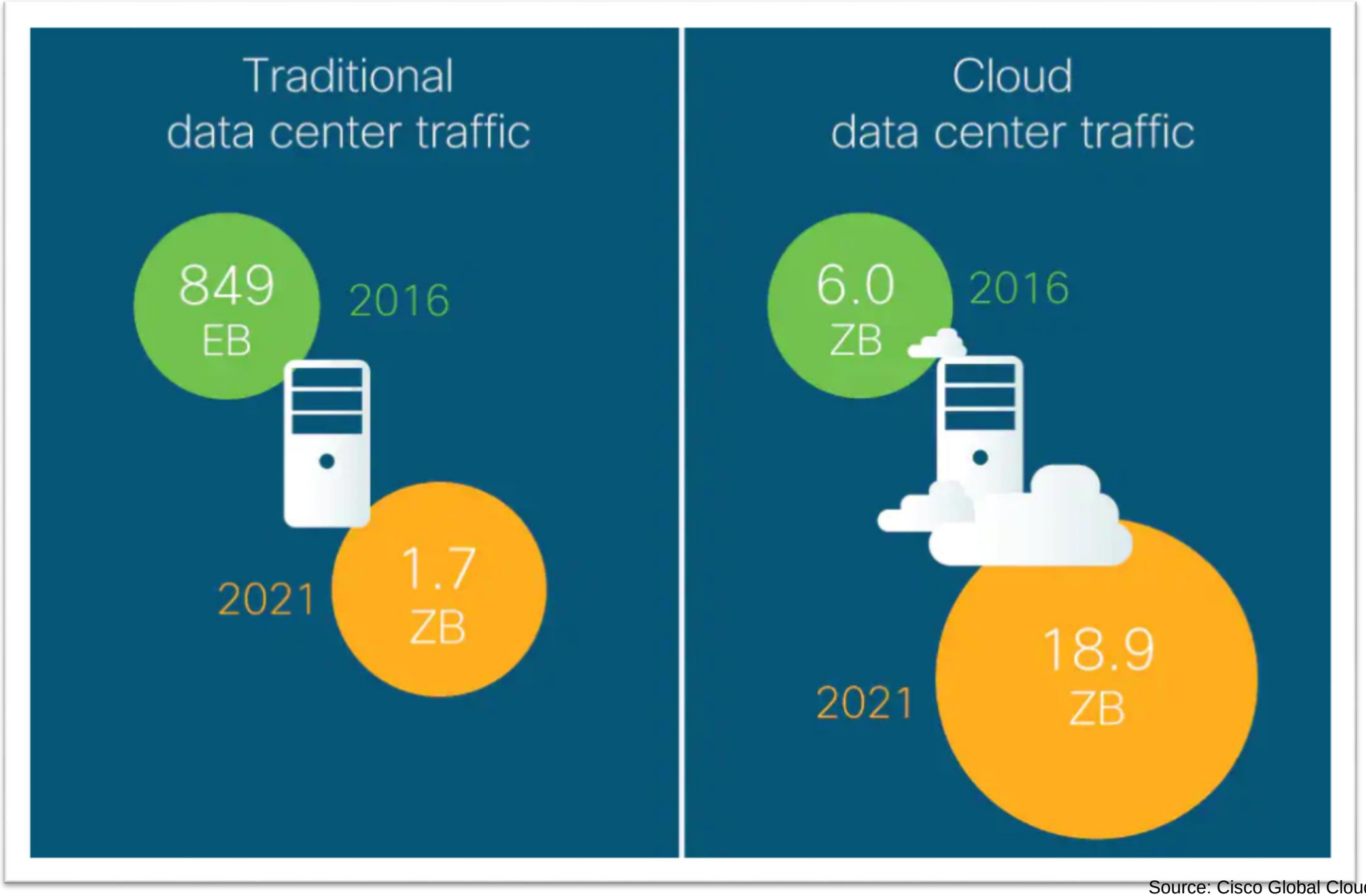
Benefit from massive economies of scale.

Stop spending money on running and maintaining data centers.

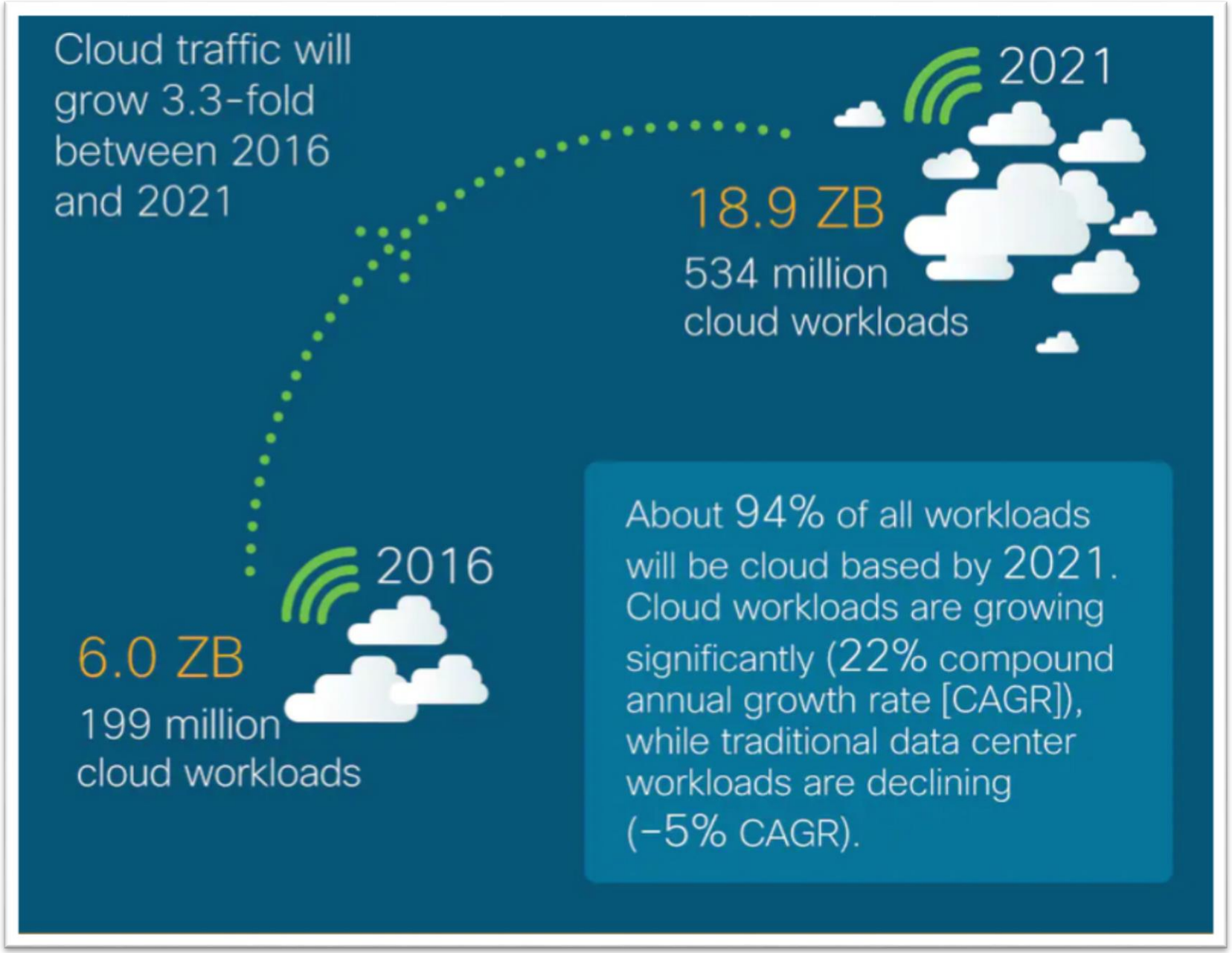


Stop guessing capacity.

Go global in minutes.



Source: Cisco Global Cloud Index (CGI)



Source: Cisco Global Cloud Index (CGI)

How Cloud may leverage your IT Resource- Quick RECAP

Enhance Business Agility	Provisioning resources in less than 5 minutes
Business Continuation	Every component of SODC will be utilized most efficiently and load balanced
Reduce IT Manageability Cost	SODC will manage the infrastructure to meet user, application & business need
Consolidation	DC Resources are optimized with scalable resource utilization
Virtualize and Automate	Virtual resource pool, quick orchestration & rapid delivery

Thank you

Hasan.Emdad@kloud.com.bd