

**«CLOUD»**

# Agenda

**Definizione di Cloud**



**La sicurezza nel Cloud**



# Cos'è il Cloud?



## La definizione di Cloud Computing

NIST: National Institute of Standard and Technology

“Il cloud computing **è un modello** abilitante un accesso comodo ed on-demand ad un **pool condiviso** di risorse di calcolo configurabili che possono essere **velocemente** ottenute e rilasciate con minimo sforzo di gestione ed una **limitata interazione** con il fornitore di servizi.”

# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

Il modello del NIST viene inquadrato come composto da:

- cinque caratteristiche essenziali;



- quattro modelli di sviluppo;



- tre modelli di servizi.



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology



### **Self service ed on-demand**

L'utente del servizio può richiedere ed utilizzare le risorse di calcolo e di storage secondo le sue necessità, senza richiedere nessuna interazione umana con il fornitore di servizi.

### **Accesso di rete aderente agli standard**

Le capacità fornite dal servizio sono disponibili sulla rete e disponibili attraverso meccanismi standard che permettono l'utilizzo ad applicazioni eseguite su piattaforme eterogenee.

# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology



### **Resource pooling**

Le risorse del fornitore di servizio sono raggruppate allo scopo di servire gli utilizzatori attraverso un modello di erogazione multi-tenant. Le risorse fisiche e virtuali sono assegnate dinamicamente secondo le esigenze degli utilizzatori. Questi ultimi non hanno visibilità dell'effettiva posizione fisica delle risorse utilizzate se non con un livello di astrazione molto elevato (nazione, stato o al massimo datacenter).

### **Elasticità**

Le risorse possono essere fornite in modo elastico, veloce e, a volte, automatico permettendo una veloce scalabilità verso l'alto e verso il basso. L'utilizzatore, potendo acquistare l'uso di risorse in qualsiasi quantità ed in qualunque momento, ha la percezione di una disponibilità potenzialmente infinita.

# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology



### **Costo commisurato all'effettivo utilizzo**

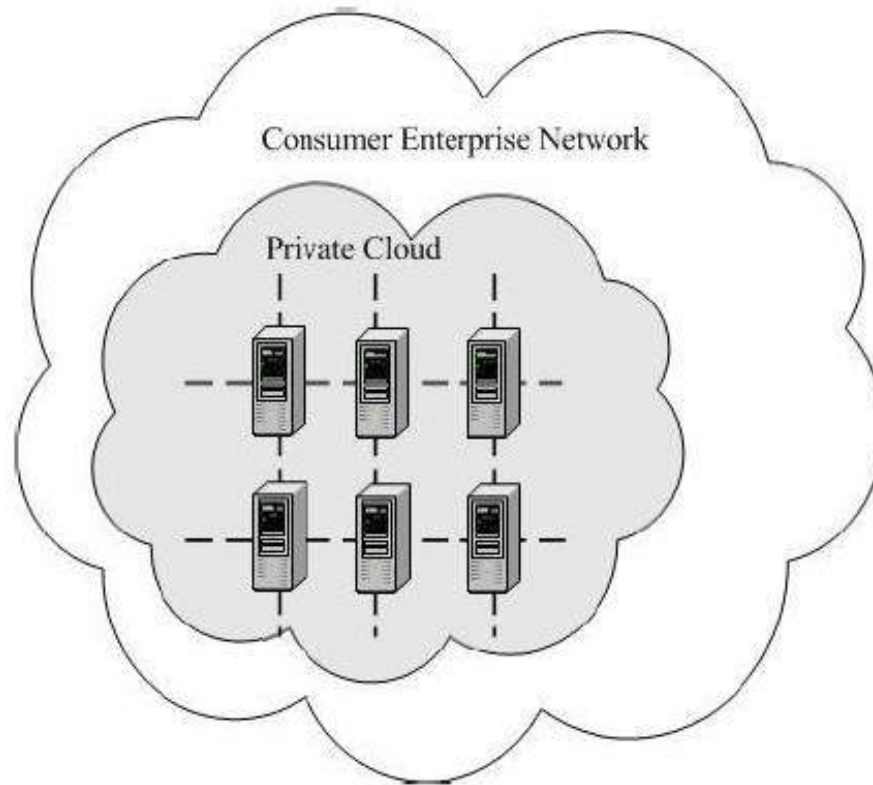
I sistemi cloud controllano ed ottimizzano automaticamente l'uso delle risorse facendo leva sulla capacità di misura dell'uso delle tipologie di servizio (es. storage, computing time, banda). L'utilizzo delle risorse può essere monitorato e controllato in modo trasparente per il fornitore di servizio e l'utilizzatore.



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

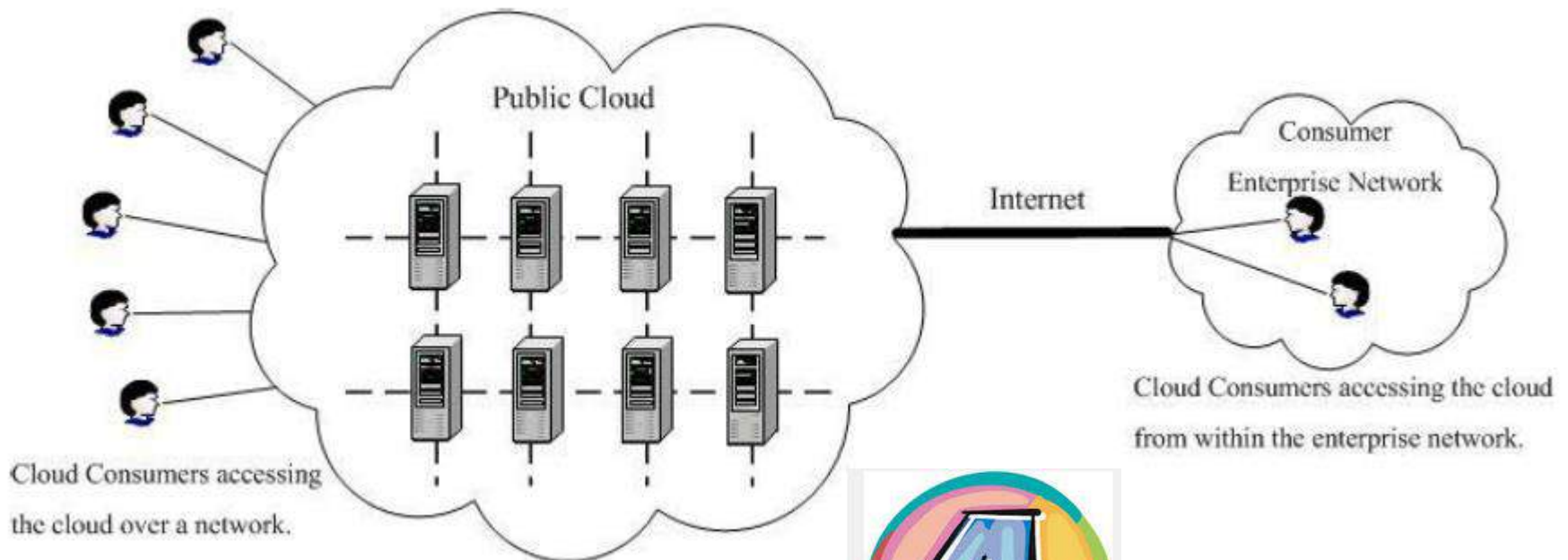
**Private Cloud:** l'infrastruttura cloud è nelle mani di un preciso responsabile sia tecnico che legale (ditta e/o persona fisica/giuridica) ed i servizi sono emessi dal cloud a precisi enti e solo ad essi.



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

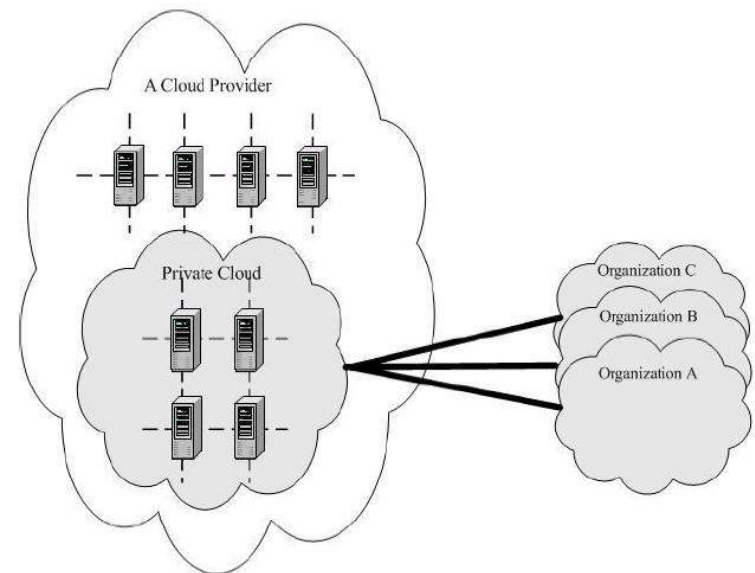
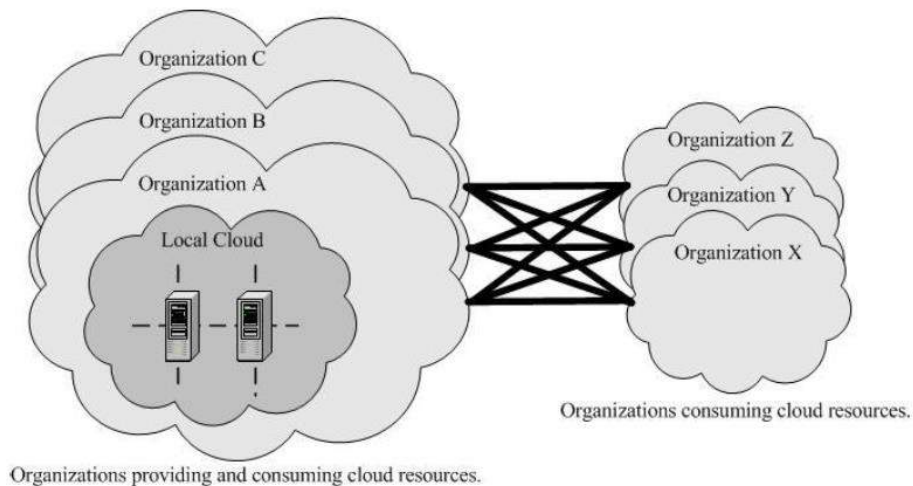
**Public Cloud:** l'infrastruttura cloud è sostenuta da ditte private, enti accademici e/o istituzionali. I servizi cloud disponibili sono venduti o resi disponibili (talvolta anche gratis) al pubblico (talvolta senza identificazione forte dell'utente).



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

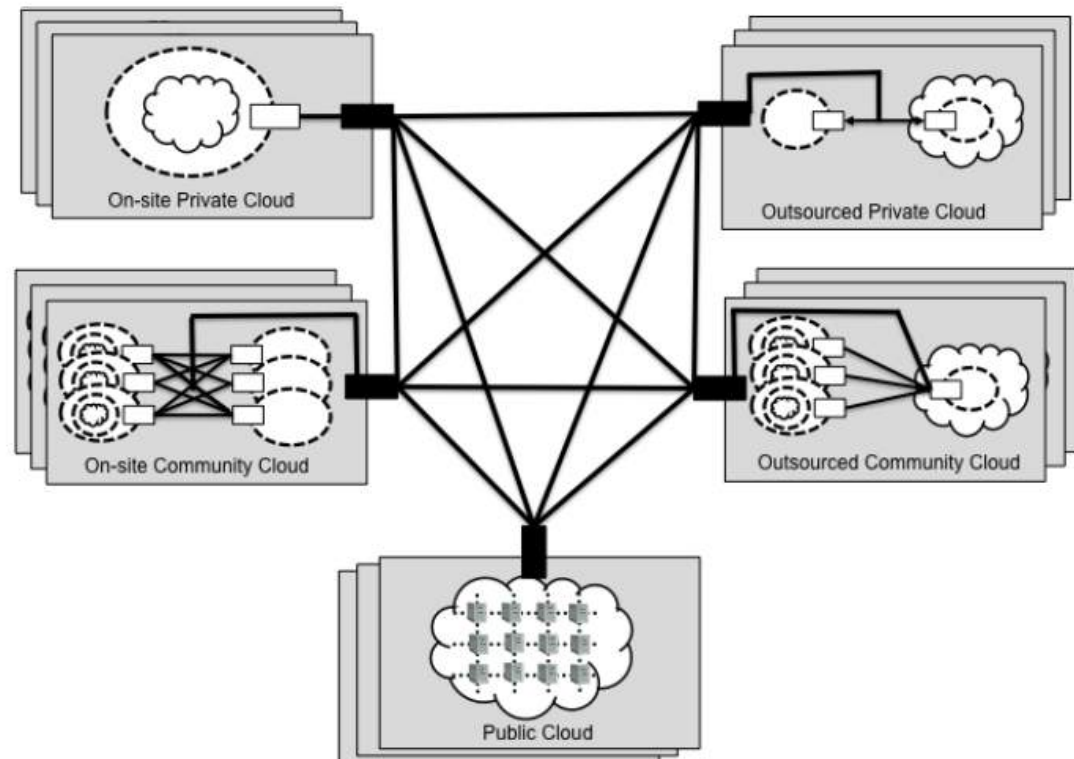
**Community Cloud:** l'infrastruttura cloud è sostenuta da un gruppo di organizzazioni che condividono missione e particolari requisiti come la sicurezza e le politiche di gestione. Gli utenti abilitati ad usufruire dei servizi fanno parte di una classe di persone ed enti/ditte.



# La definizione di Cloud Computing

NIST: National Institute of Standard and Technology

**Hybrid Cloud:** l'infrastruttura cloud si compone da una o più tipologie delle precedenti. Queste mantengono le loro peculiarità ma si compongono così da generare una miriade di servizi finali, alcuni gratis, altri a pagamento, alcuni sicuri e garantiti, altri assolutamente inaffidabili ma comunque con molto richiamo sul pubblico.



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology



Il **NIST** identifica **tre tipologie di servizio**:

**Software as a Service (SaaS)**: il cliente utilizza via rete le applicazioni offerte dal fornitore in remoto, e non ha il controllo dell'infrastruttura sottostante il livello applicativo, anche se può talvolta disporre di possibilità limitate di configurazione.

**Platform as a Service (PaaS)**: il cliente può dispiegare le proprie applicazioni sull'infrastruttura fornita, nei limiti consentiti dal fornitore. Non ha controllo sull'infrastruttura sottostante, ma può controllare le applicazioni e configurare l'ambiente applicativo.

**Infrastructure as a Service (IaaS)**: il cliente controlla le risorse di elaborazione, archiviazione, rete e calcolo. Non ha la gestione né il controllo dell'infrastruttura cloud sottostante, ma può modificare entro limiti prestabiliti la configurazione e la capacità complessiva del sistema.

# La definizione di Cloud Computing

NIST: National Institute of Standard and Technology

3



"IaaS"

Infrastructure-as-a-Service

host

host

infrastructure-as-a-service



"PaaS"

Platform-as-a-Service

build

build

platform-as-a-service



"SaaS"

Software-as-a-Service

consume

consume

software-as-a-service

# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

3

### SaaS services:

- o *Email and Office Productivity*: Applications for email, word processing, spreadsheets, presentations, etc.
- o *Customer Relationship Management (CRM)*: CRM applications that range from call center applications to sales force automation.
- o *Document Management*: Applications for managing documents, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
- o *Financials*: Applications for managing financial processes ranging from expense processing and invoicing to tax management.
- o *Human Resources*: Software for managing human resources functions within companies.
- o *Sales*: Applications that are specifically designed for sales functions such as pricing, commission tracking, etc.
- o *Enterprise Resource Planning (ERP)*: Integrated computer-based system used to manage internal and external resources, including tangible assets, financial resources, materials, and human resources.



# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

3

### **PaaS Services:**

- o *Business Intelligence*: Platforms for the creation of applications such as dashboards, reporting systems, and data analysis.
- o *Database*: Services offering scalable relational database solutions or scalable non-SQL datastores.
- o *Development and Testing*: Platforms for the development and testing cycles of application development, which expand and contract as needed.
- o *Application Deployment*: Platforms suited for general purpose application development. These services provide databases, web application runtime environments, etc.





# La definizione di Cloud Computing

## NIST: National Institute of Standard and Technology

# 3

### IaaS Services:

- o *Backup and Recovery*: Services for backup and recovery of file systems and raw data stores on servers and desktop systems.
- o *Compute*: Server resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- o *Content Delivery Networks (CDNs)*: CDNs store content and files to improve the performance and cost of delivering content for web-based systems.
- o *Services Management*: Services that manage cloud infrastructure platforms. These tools often provide features that cloud providers do not provide or specialize in managing certain application technologies.
- o *Storage*: Massively scalable storage capacity that can be used for applications, backups, archival, and file storage.



# La definizione di Cloud Computing

NIST: National Institute of Standard and Technology



Vengono individuate le cinque seguenti caratteristiche essenziali: on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.

Sotto il profilo dei modelli organizzativi, si distingue fra Private cloud, Community cloud, Public cloud e Hybrid cloud.



Le modalità con cui i servizi cloud possono essere realizzati vengono invece distinte fra Software as a Service (SaaS), Platform as a Service (PaaS), ed Infrastructure as a Service (IaaS).

# La Sicurezza nel Cloud Computing

## Agenda

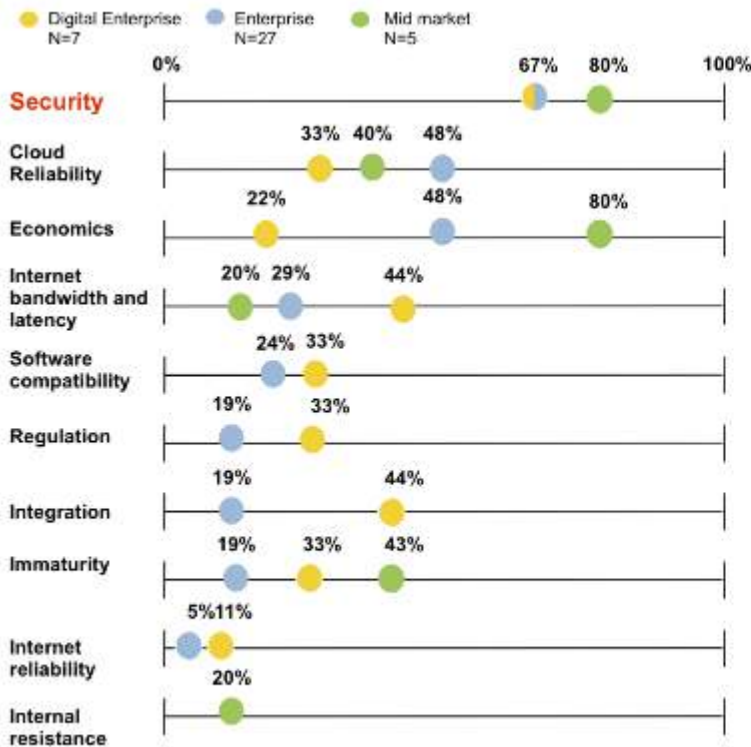
- Cloud Security: problemi e rischi
- Come rendere sicuro il cloud computing
- Sicurezza nei diversi modelli di Cloud
- Conclusioni



# La Sicurezza nel Cloud Computing

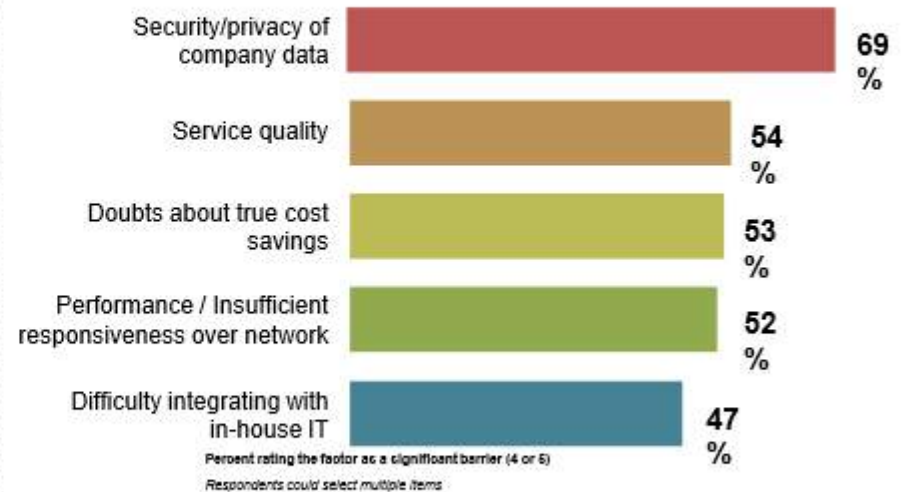
## Cloud security: problemi e rischi

Recenti studi mostrano che la sicurezza è il principale inibitore per le aziende nell'adozione delle tecnologie cloud.



Source: Oliver Wyman Interviews

Quali sono percepite come barriere attuali o potenziali per l'acquisizione di servizi public cloud ?

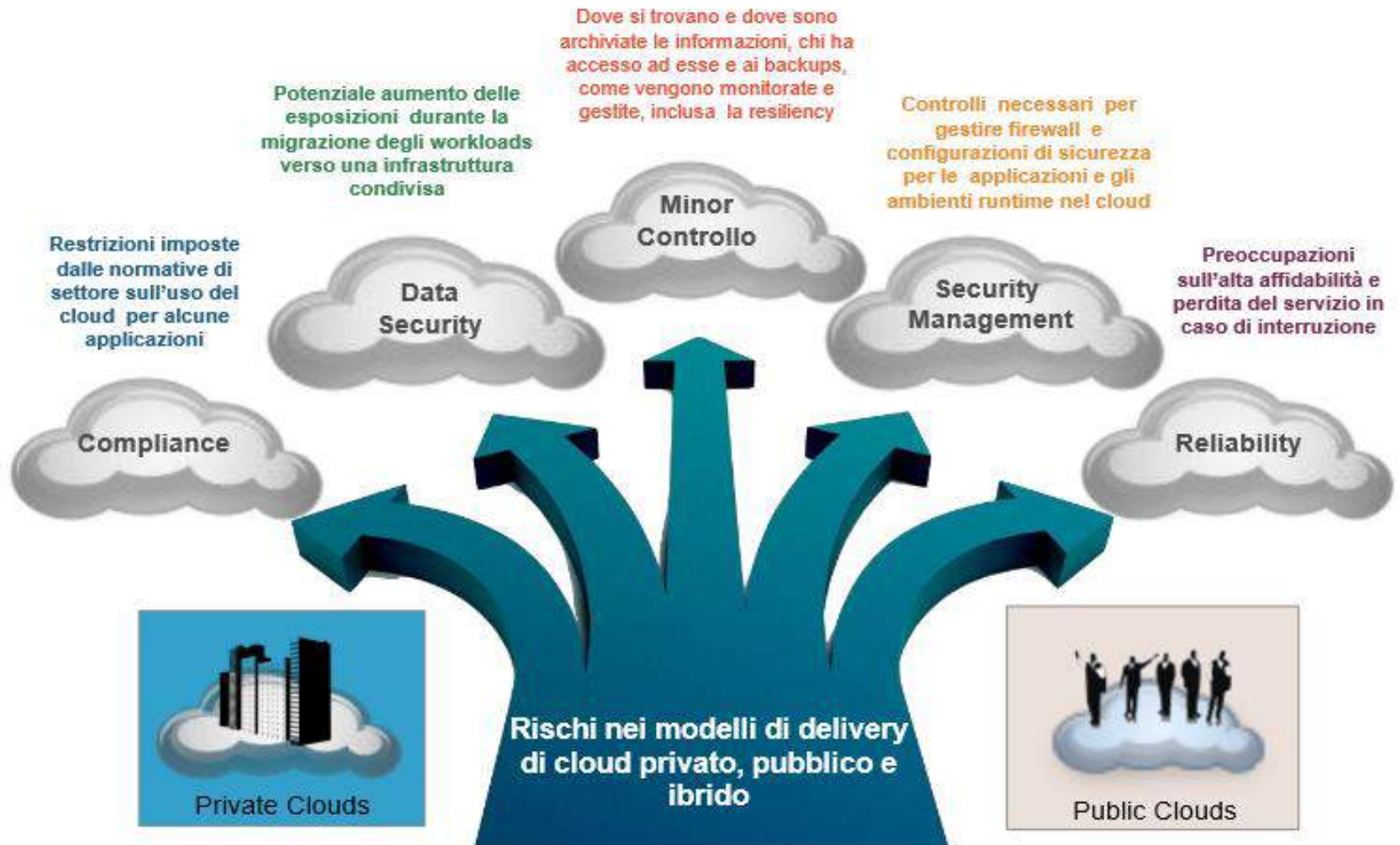


Source: IBM Market Insights, Cloud Computing Research, July 2009, n=1,000

# La Sicurezza nel Cloud Computing

## Cloud security: problemi e rischi

### I rischi introdotti con il cloud computing



# La Sicurezza nel Cloud Computing

## Cloud security: problemi e rischi



### Security and Privacy Domains

People and Identity

Data and Information

Application and Process

Network, Server and Endpoint

Physical Infrastructure

Governance, Risk and Compliance



Multiple Logins, Onboarding Issues

Multi-tenancy, Shared Resources

External Facing, Quick Provisioning

Virtualization, Reduced Access

Provider Controlled, Lack of Visibility

Audit Silos, Logging Difficulties

In un ambiente cloud, gli accessi si ampliano, le responsabilità e i controlli cambiano, ed aumenta la velocità del provisioning delle risorse e delle applicazioni – **con impatti su tutti gli aspetti della sicurezza IT.**

# La Sicurezza nel Cloud Computing

Caratteristiche legate alla sicurezza nei diversi modelli di Cloud



## Private cloud

Infrastrutture cloud (on o off site) utilizzate esclusivamente per un'azienda e gestiti dall'organizzazione stessa o da una terza parte



## Community cloud

L'infrastruttura cloud è sostenuta da un gruppo di organizzazioni che condividono missione e particolari requisiti come la sicurezza e le politiche di gestione



## Public cloud

A disposizione del pubblico in generale o di un grande gruppo industriale e di proprietà di una organizzazione di vendita di servizi cloud



- Cliente responsabile dell'infrastruttura
- Maggior personalizzazione dei controlli di sicurezza
- Buona visibilità delle operazioni day-to-day
- Facilità di accesso a logs e policies

- Fornitore responsabile dell'infrastruttura
- Minor personalizzazione dei controlli di sicurezza
- No visibilità delle operazioni day-to-day
- Difficoltà di accesso a logs e policies

# La Sicurezza nel Cloud Computing

## Come rendere sicuro il cloud computing

L'approccio e' quello di sviluppare la sicurezza in linea con ogni fase di un progetto o di una iniziativa cloud



### Design

Definire la strategia e il piano d implementazione per migrare in cloud.



### Deploy

Costruire servizi cloud , per l'azienda e/o come cloud services provider.



### Consume

Gestire e ottimizzare consumi di servizi cloud.

#### Cloud Security Approach

#### **Secure by Design**

*Focus sull'inclusione della security nella costruzione del cloud.*

#### **Workload Driven**

*Rendere sicure le risorse cloud con features e prodotti innovativi.*

#### **Service Enabled**

*Governare il cloud attraverso la gestione della sicurezza e degli workflow.*

#### Example security capabilities

- Cloud security roadmap
- Network threat protection
- Server security
- Database security

- Application security
- Virtualization security
- Endpoint protection
- Configuration and patch management

- Identity and access management
- Secure cloud communications
- Manage and monitor security



# La Sicurezza nel Cloud Computing

## Sicurezza nei diversi modelli di Cloud

**Infrastructure as a Service (IaaS):** Ridurre i costi e la complessità dell'IT attraverso cloud data centers

### Cloud Enabled Data Center

*Integrated service management, automation, provisioning, self service*

Key security focus:  
**Infrastructure**

- Manage datacenter identities
- Secure virtual machines
- Patch default images
- Monitor logs on all resources
- Defend network threats



**Platform-as-a-Service (PaaS):** Accelerare time to market con servizi di piattaforma in cloud

### Cloud Platform Services

*Pre-built, pre-integrated IT infrastructures tuned to application-specific needs*

Key security focus:  
**Data and Information**

- Secure shared databases
- Encrypt private information
- Build secure applications
- Keep an audit trail
- Integrate existing security



**Innovare i business models** diventando un cloud service provider

### Cloud Service Provider

*Advanced platform for creating, managing, and monetizing cloud services*

Key security focus:  
**Governance and Compliance**

- Isolate cloud tenants
- Secure portals and APIs
- Manage security operations
- Build compliant data centers
- Offer backup and resiliency



**Software as a Service (SaaS):** Ottenere accesso immediato ad applicazioni di business on cloud

### Business Solutions on Cloud

*Capabilities provided to consumers for using a provider's applications*

Key security focus:  
**Applications and Identity**

- Harden exposed web apps
- Securely federate identity
- Deploy access controls
- Encrypt communications
- Manage application policies



# La Sicurezza nel Cloud Computing

## Conclusioni

Il Cloud Computing sta accelerando il modo in cui le aziende proteggono le loro informazioni critiche, spostando il focus dalla sicurezza dell' endpoint e della rete, ad una **protezione olistica** dei dati

Garantire la sicurezza negli ambienti Cloud richiede specifiche:

- Metodologie , Processi e organizzazione
- Infrastrutture
- Competenze e Certificazioni
- **Service Level Agreements**



Il Cloud può risultare più sicuro degli ambienti tradizionali, per i seguenti motivi:

- ✓ Servizi di sicurezza specializzati per gli workload
- ✓ Maggiori risorse per la sicurezza
- ✓ Security as Service: **le migliori tecnologie** ad un costo sostenibile
- ✓ Competenze

# Cloud Computing

## Video

## Ulteriori evoluzioni tecnologiche Hyper-converged infrastructure

# Convergence

**A service, not an architecture**

**Integration**



**+ Single source support**



**Servers, switches, storage, and software from multiple vendors, racked, cabled and integrated before delivery. Supported by a single organization.**



**Network**

**Compute**

**Storage**

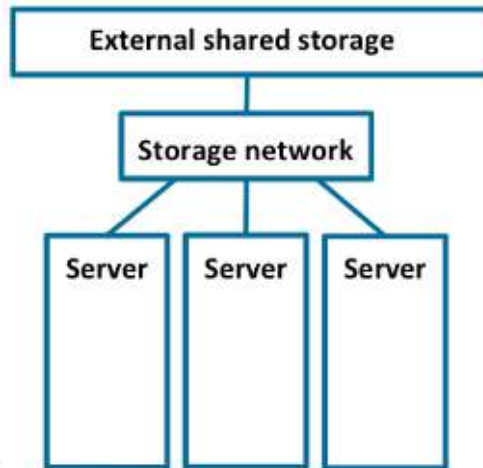
# Ulteriori evoluzioni tecnologiche

## Hyper-converged infrastructure

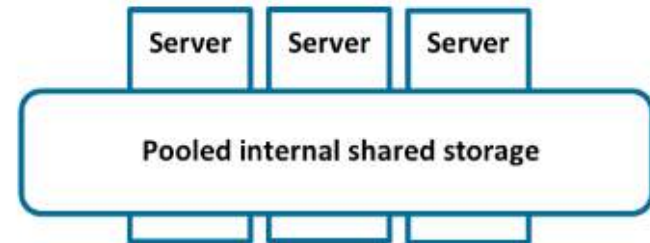
# Hyper-convergence

[noun] [*hahy-per*] [*kuh n-vur-juh ns*]: An IT infrastructure architecture in which compute and shared storage are provided from the same hardware – usually a cluster of virtualized servers

## Conventional



## Hyper-converged



# 1. Hyper-Converged tradizionale

Utilizzo di hardware tradizionale gestito dallo strato software del virtualizzatore (vmware o hyper-v)



- EVO RAIL (hp, dell, fujitsu, EMC2, hitachi, inspur, supermicro)

- Dell CPS



- «Lego system»: gestione hardware interna



- EMC2 ScaleIO: gestione hardware interna



## Considerazioni

### PRO:

- Basso costo dell'hardware (tranne che per Dell CPS)
- Per «Lego System» e ScaleIO: Possibilità di espansione secondo due direzioni indipendenti: computing o storage
- Per «Lego System»: indipendenza soluzione di virtualizzazione
- Immediata possibilità di espansione verso i Cloud Provider
- SSDC ready

### CONTRO:

- Limitazioni sulla crescita (solo per EVO RAIL)
- Limite su max RAM per appliance inferiore all'attuale (maggiore spazio CED occupato, solo EVO RAIL)
- Maggiore effort delle risorse professionali (in particolare per «Lego System»)
- Dell CPS disegnata per Microsoft
- ScaleIO: costi licenze sw aggiuntivi

## 2. Hyper-Converged ibrido

Soluzioni all-in-one, con utilizzo di hardware proprietario Cisco gestito dallo strato proprietario integrato con vmware

- Cisco + Simplivity (OmniStack)



### Considerazioni

#### PRO:

- Soluzione chiavi in mano per il mondo virtuale
- Possibilità riciclo hardware
- Deduplica nativa (elevate prestazioni)
- Supporto nativo per soluzioni:
  - DR
  - BC
  - Backup
  - Stretched Cluster

#### CONTRO:

- Al momento supporto solo per vmware
- Presenza in Italia limitata
- Costo elevato

### 3. Hyper-Converged puro

Soluzioni black-box, con utilizzo di hardware proprietario gestito da software proprietario

- Nutanix



#### Considerazioni

##### PRO:

- Soluzione chiavi in mano per il mondo virtuale
- Minimo effort risorse professionali
- Supporto nativo per soluzioni:
  - DR
  - BC
  - Backup (proprietario)
  - Stretched Cluster

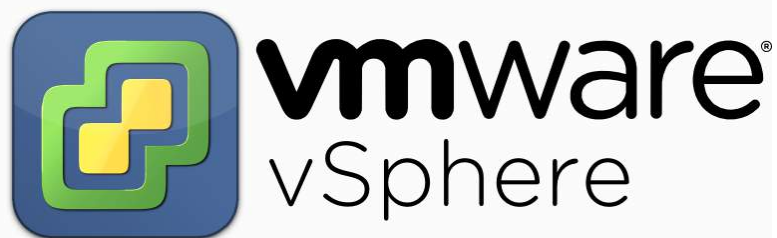
##### CONTRO:

- Solo per applicazioni ad alte prestazioni
- Presenza in Italia limitata
- Costo elevato
- Lock-in con il vendor



# Ulteriori evoluzioni tecnologiche

## Il governo dell'infrastruttura da parte dei Virtualizzatori



## Service Delivery

Business Relationship Management

Capacity Management

Availability and Continuity Management

Information Security Management

Regulatory Policy and Compliance Management

Financial Management

Service Level Management

Service Lifecycle Management

Define

Enable services

Define

Enable services

Define

Software

Provide capability

Platform

Provide capability

Infrastructure

Virtualization

Compute

Network

Storage

Manage and support

Provide capability

Management and Support

Consumer and Provider Portal

Usage and Billing

Service Reporting

Service Monitoring

Service Management

Configuration Management

IT Automation

Infrastructure Capacity

Application Test

Data Protection

Application Deployment

Application Release

Server Conf. Provisioning

Network Support

Define

Support

Service Operations

Request Fulfillment

Access Management

Asset and Configuration Management

System Administration

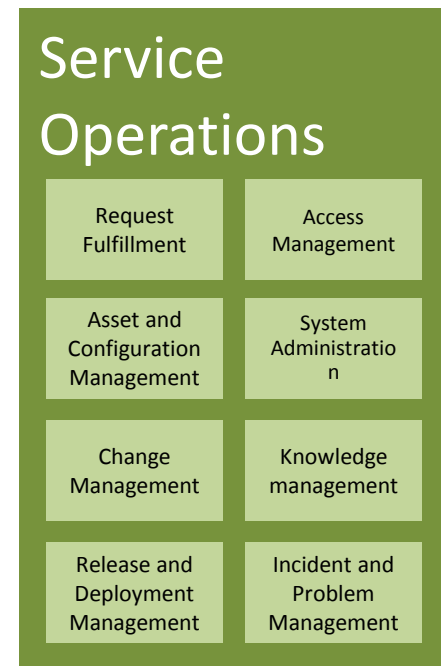
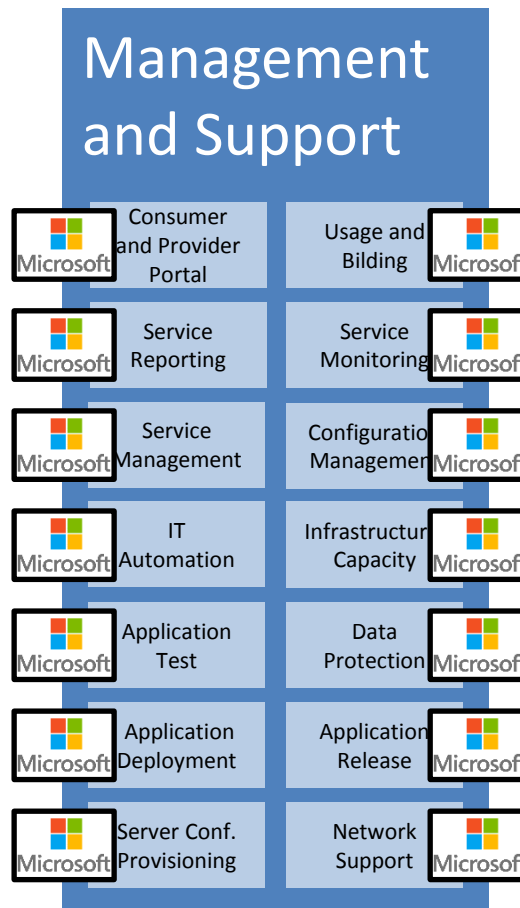
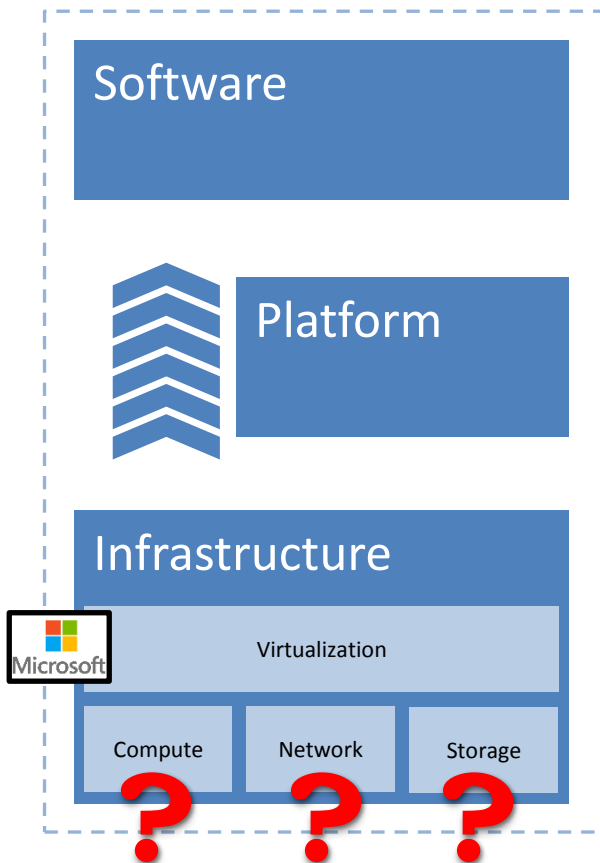
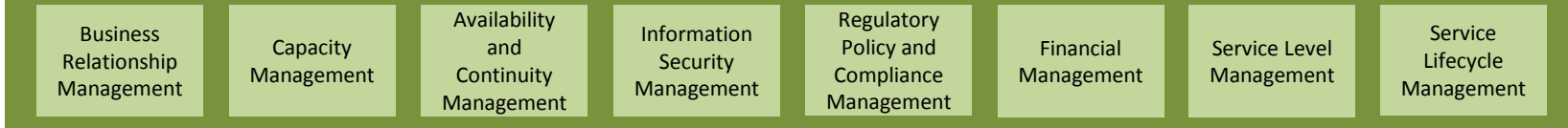
Change Management

Knowledge management

Release and Deployment Management

Incident and Problem Management

## Service Delivery



# Seed Blueprint

AREA	SC SERVICE MANAGER	SC VIRTUAL MACHINE MANAGER	SC CONFIGURATION MANAGER	SC OPERATION MANAGER	SC DATA PROTECTION MANAGER	SC ORCHESTRATOR / SMA	WINDOW S AZURE PACK	TEAM FOUNDATION SERVER
CMDB	✓							
Asset Discovery			✓					
Trouble Ticketing	✓							
Knowledge Error	✓			✓				
Network Monitoring				✓				
System Monitoring				✓				
Application Monitoring				✓				
Application Release		✓	✓			✓		✓
Job Scheduling						✓		
Application Test & Performance				✓				✓
Infrastructure Change	✓	✓	✓	✓		✓		
Infrastructure Capacity	✓	✓		✓				
Service Reporting	✓	✓		✓				
Server Configuration & Provisioning	✓	✓	✓			✓	✓	
IT Automation	✓	✓	✓			✓	✓	
Data Protection					✓			



PEOPLE