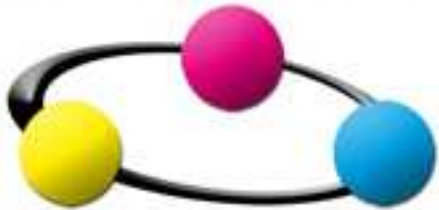


SECURITY



SUMMIT

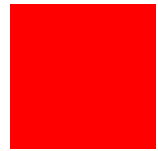
**Security Summit 2010 – Roma**

**Oracle** Community For Security

**Il Cloud Computing: nuovo paradigma e nuovi rischi?**

Valentino Squilloni - Reply





# Agenda



- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing





# Agenda



- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

# Definizioni



Cloud computing is a style of computing where **massively scalable** IT-related capabilities are provided **'as a service'** across the **Internet** to multiple external customers.

Fonte: Gartner

**Scalabilità massiva:** flessibile ed adatto a clienti di ogni dimensione

**'as a service':** funzionalità pay-per-use regolate da SLA

**Standard specifici:** semplicità d'uso

Il Cloud è un modello che supporta quello che viene chiamato **ADAM** (Alternative Delivery and Acquisition Model) in cui ogni cosa (**XaaS**), e non solo un software, può essere offerta "a servizio"

# NIST Visual Model



*NIST - National Institute of Standards and Technology*

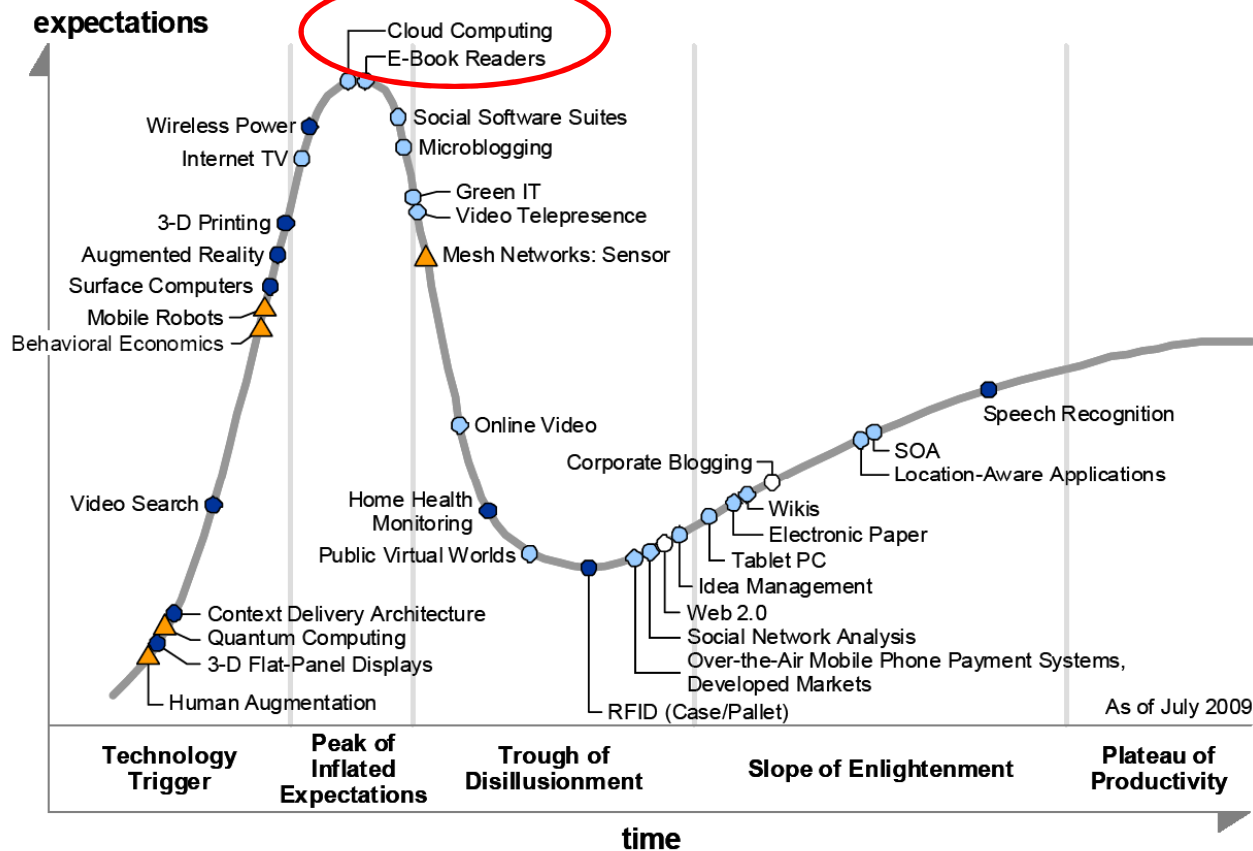
<http://csrc.nist.gov/groups/SNS/cloud-computing/>

**Oracle** Community For Security



# Hype Cycle – Emerging Technologies

Figure 1. Hype Cycle for Emerging Technologies, 2009



Years to mainstream adoption:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

Source: Gartner (July 2009)

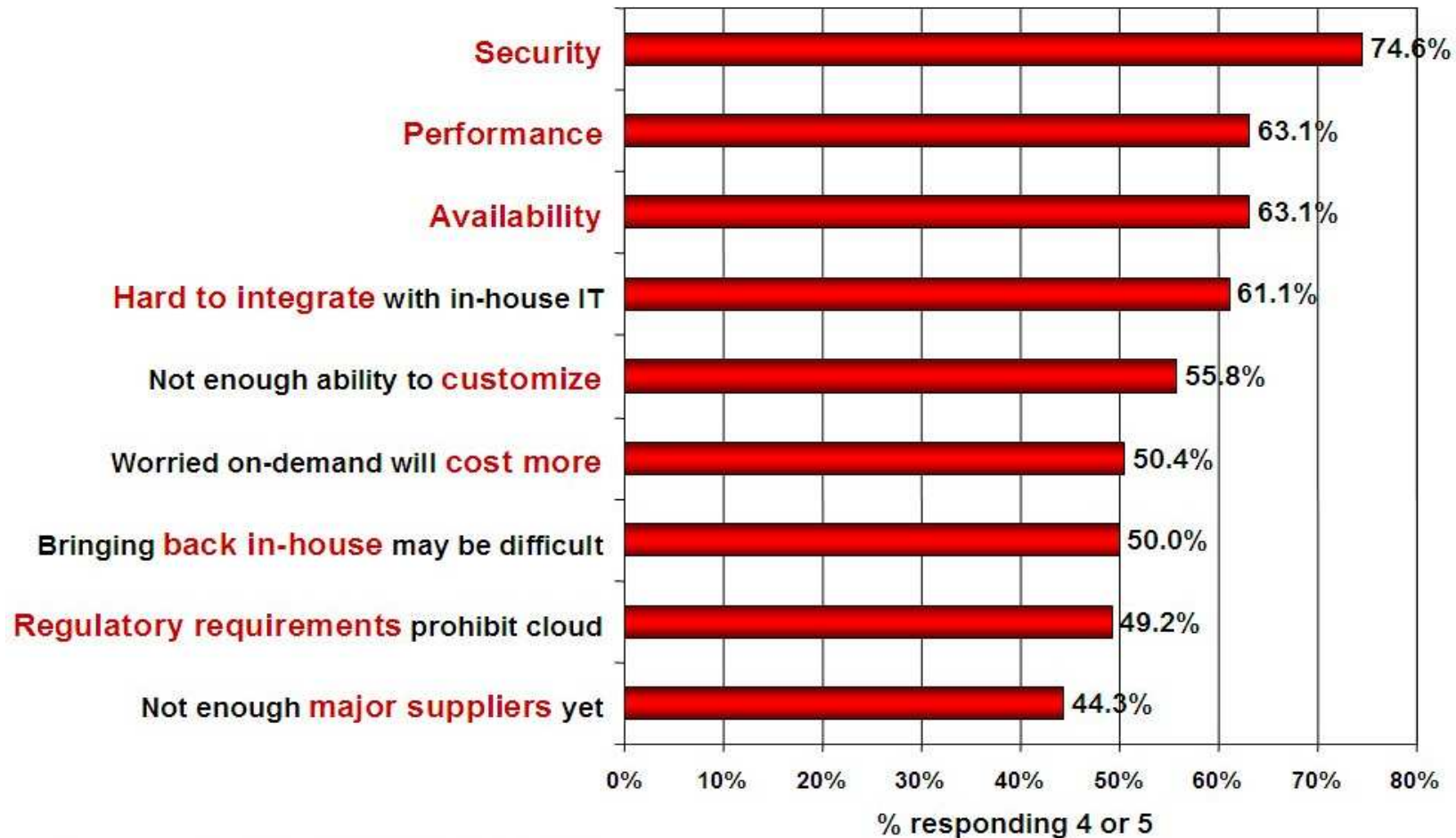


# Agenda



- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

# Cloud Computing issues



Source: IDC Enterprise Panel, August 2008 n=244

Oracle Community For Security



# Rischi e i Controlli di Sicurezza nel Cloud Computing



- **ENISA** – tipologie di rischi del Cloud Computing:
  - Cloud Computing - Benefits, risks and recommendations for information security (ENISA, Nov. 09)
- **Cloud Security Alliance (CSA)** – controlli di sicurezza da effettuare su ambienti Cloud:
  - Security Guidance for Critical Areas of Focus in Cloud Computing (CSA, Dic. 09)

# ENISA – Categorie di rischio



# CSA – Domini di controllo



- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability

**DOMINI DI  
GOVERNO**

**DOMINI DI  
TECNOLOGICI**

- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

# Approccio per la gestione della sicurezza



## Valutazione del rischio

- Utilizzare una metodologia specifica per un ambiente Cloud



## Identificare le azioni per mitigare il rischio

- Soluzioni tecniche (Es. Cifratura File System)
- Soluzioni organizzative (Es: definizione dei processi amministrativi)



## Misurazione del rischio residuo



## Accettazione del rischio



# Agenda



- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

# Mitigare i rischi del cloud



- La sicurezza IT dipende da persone, processi e tecnologia
- Quali sono le soluzioni tecnologiche disponibili ad oggi per mitigare i rischi evidenziati finora nel cloud?
- Focus on:
  - Data Encryption & Key Management nel Cloud (Dominio **Encryption and Key Management**)
  - Federated Identity nel Cloud (Dominio **Identity and Access Management**)

# Riservatezza dati su Cloud



- **Quali sono le soluzioni di mitigazione per garantire la riservatezza dei dati su Cloud?**
  - Focalizziamo gli esempi sulle infrastrutture IaaS (le soluzioni possono essere traslate nelle modalità di erogazione PaaS e SaaS)
- **Quali sono i rischi che cerchiamo di mitigare?**
  - Cloud provider malicious insider - abuse of high privilege roles
  - Intercepting data in transit
  - Data leakage on up/download, intra-cloud
  - Insecure or ineffective deletion of data
  - Loss of encryption keys

# La crittografia dei dati



- Nei ToS di Amazon AWS è presente la seguente clausola:
- **“YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA.”**
- “You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you.”

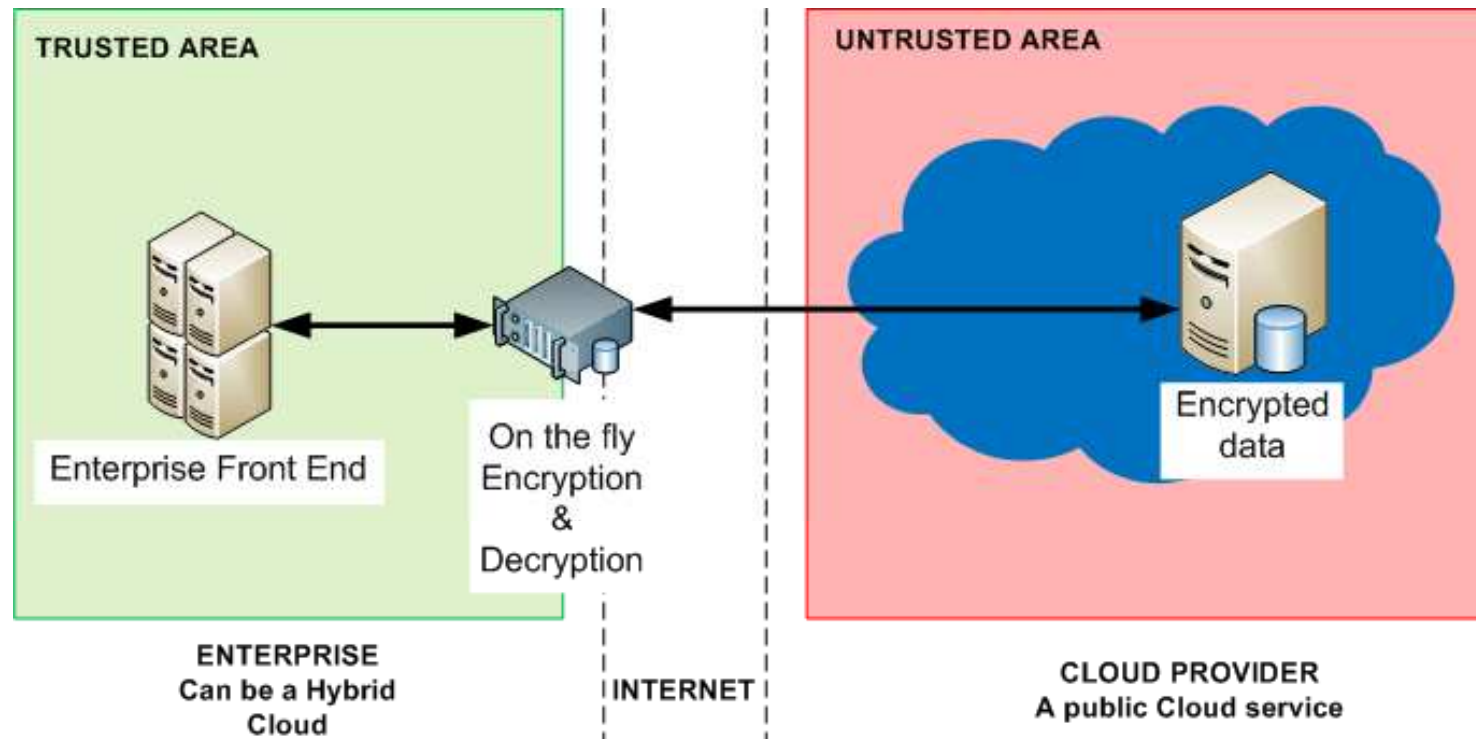
... un messaggio chiaro

# La gestione delle chiavi



- La crittografia dei dati è una delle possibili soluzioni. Il problema delle infrastrutture Cloud è: come gestiamo le chiavi?
- Ad oggi a responsabilità della gestione delle chiavi (storage e provisioning) è del Cliente
- Nessun Cloud Services Provider ad oggi mette a disposizione tecnologie HSM, per definizione 'non virtualizzabili' e gli standard (PKCS10/11) non sono adatti ad utilizzi in ambito Cloud
- Usare la crittografia per evitare l'accesso ai dati da parte del Cloud Provider è complesso

# Soluzioni disponibili



- Encryption si applica ai dati significativi (es: anagrafiche) sia 'at rest' che 'in motion'
- Le chiavi sono gestite 'off-cloud'

# Altre soluzioni possibili per la data encryption



- **Fidarsi del Cloud Provider (es: Amazon)**
  - Alcune domande da fare:
    - Quali sono i modelli di sicurezza del Cloud Provider?
    - Come gestisce gli accessi alle informazioni?
    - Quali sono gli SLA? Che garanzie offrono in caso di accesso non autorizzato?
    - Che strumenti di monitoraggio vengono utilizzati per rilevare accessi non desiderati?
    - Sussistono obblighi di comunicazione verso l'Enterprise dei security breach che coinvolgono i loro dati?
  - Questa soluzione prevede che il Cloud Provider abbia potenzialmente accesso sia alle chiavi dunque anche ai dati (sia nel caso di cifratura dei dati 'at rest' che 'in motion')
- **Utilizzare delle 'secure area' fornite sul Cloud dal Provider all'Enterprise per la gestione delle chiavi ('Virtual HSM')**
  - Una soluzione futuribile più che una realtà

# La gestione delle identità



- **L'Identity Management su Cloud è un tema critico**
- Come faccio a:
  - Far risiedere gli account nell'Enterprise e allo stesso tempo autenticare autorizzare gli stessi account su Cloud?
  - Per ridurre la superficie di esposizione ad attacchi, come faccio a far gestire l'inserimento di username e pwd (in caso di utenti fisici) nel perimetro dell'Enterprise?
- **La soluzione: Federated Identity Management**
- Cos'è?
  - Un sistema che permette a un individuo di utilizzare username, password o altre componenti di identificazione per autenticarsi su diversi network di enterprise differenti
- **Quali sono i rischi che cerchiamo di mitigare?**
  - Cloud provider malicious insider - abuse of high privilege roles
  - Compliance challenges
  - Loss of governance
  - Privilege escalation
  - Risk from changes of jurisdiction
  - Data protection risks



# Agenda



- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

# Il Cloud può portare benefici di sicurezza?



- **I benefici di business sono chiari**
  - CAPEX->OPEX
  - Immediatezza e disponibilità, facilità d'uso
  - Scalabilità, efficienza, resilienza
- **Ma esistono dei rischi:**
  - Abbiamo parlato di rischi e corretta gestione degli aspetti di sicurezza utilizzando un approccio strutturato "Risk Based"
- **Il Cloud può portare reali benefici dal punto di vista della sicurezza?**
  - E' possibile, applicando economia di scala alle soluzioni di sicurezza
- **Come ogni benchmark, dipende dallo stato attuale REALE della gestione della sicurezza dell'Enterprise**
  - Quali sono le attuali politiche di patch management?
  - Quanto sono distribuiti di dati?
  - Quale è la periodicità delle verifiche di sicurezza?
  - Etc. etc.

# I principali benefici di sicurezza



- **L'ENISA definisce i seguenti benefici assoluti:**
  - Security and the benefits of scale
  - Security as a market differentiator
  - Standardized interfaces for managed security services
  - Rapid, smart scaling of resources
  - Audit and evidence-gathering
  - More timely, effective and efficient updates and defaults
  - Benefits of resource concentration
- **I reali benefici per l'enterprise possono essere di due tipologie:**
  - Concreto risparmio nella gestione della sicurezza e cost accounting
  - Miglioramento dello stato di sicurezza per processi parzialmente presidiati

# I principali benefici di sicurezza



- Due esempi:
- **Concreto risparmio nella gestione della sicurezza**
  - In una soluzione SaaS le attività di patch management e di vulnerability management sono a carico del fornitore del servizio e possono essere regolati da SLA
  - Spesso tali costi non sono internamente direttamente ripartiti sui servizi, rendendo difficile la valutazione economica del beneficio di esternalizzare un servizio di sicurezza
- **Miglioramento dello stato di sicurezza per processi parzialmente presidiati**
  - Se le analisi dello stato attuale evidenziano una esposizione al rischio elevata, una migrazione ad una situazione di rischio moderato, su Cloud, rappresenta un miglioramento.
  - Inoltre il cambio di paradigma di erogazione costringe l'Enterprise a riconsiderare tutti gli aspetti di gestione della sicurezza per il sistema specifico, facendo spesso emergere situazioni non gestite o parzialmente presidiate

# Conclusione



- Abbandonate i preconcetti che avete sulla sicurezza dei servizi Cloud:
- La sicurezza può
  - Essere misurata
  - Essere gestita
  - Migliorare rispetto ad uno stato attuale
  - Costare meno
  - .....

....GRAZIE!