cloud security alliance

Securing the Present and Future of Cloud Computing

Jim Reavis, Executive Director

December, 2009

Cloud Computing: Real or Hype?

- Both!
- Next Phase of the Internet
  - Early ‘90s – Mid ‘00s: Compute Connectivity
  - Mid ‘00s – Mid ‘20s: Compute Utility
- Overhyped in the short term, underhyped in the long term
- Opportunity for enterprises to disrupt the balance of power OR have new benevolent overlords

What has driven Cloud Computing?

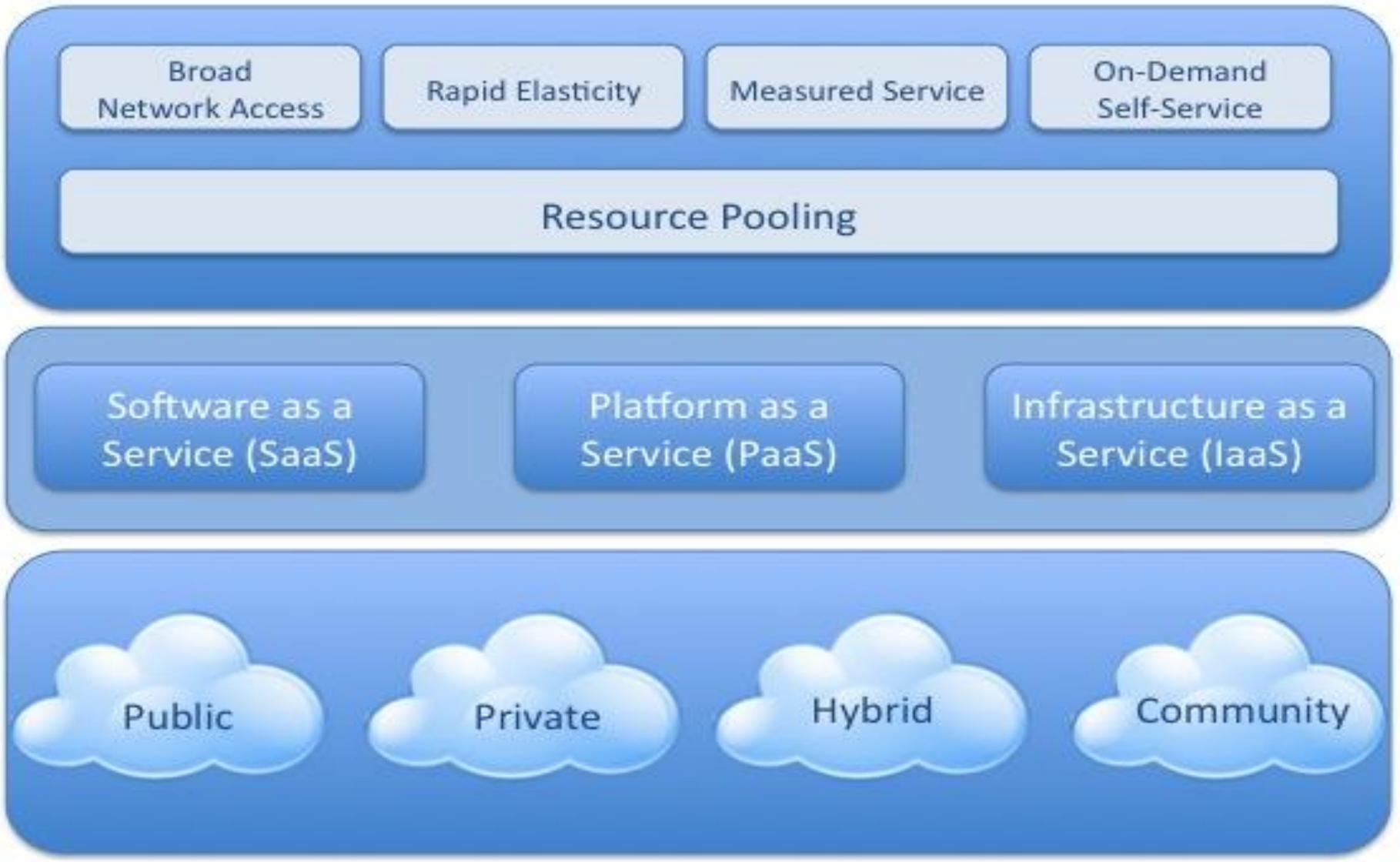
- Hyperconnectivity: massive DotCom infrastructure investments
- Moore's Law: driving costs of compute & storage towards zero
- Service Oriented Architecture: self-describing protocols democratize applications
- Scale: major providers mastering complexity of delivering massive scale, creating the argument of economy

What is Cloud Computing?

- On demand model for allocation and consumption of computing as a utility
  - Immediacy
  - Elasticity
  - Multi-tenancy
- NIST Definition becoming pervasive
  - Infrastructure as a Service (IaaS): basic O/S & storage
  - Platform as a Service (PaaS): IaaS + development environment
  - Software as a Service (SaaS): complete application
  - Public, Private, Community & Hybrid Cloud deployments

What is Cloud Computing?

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

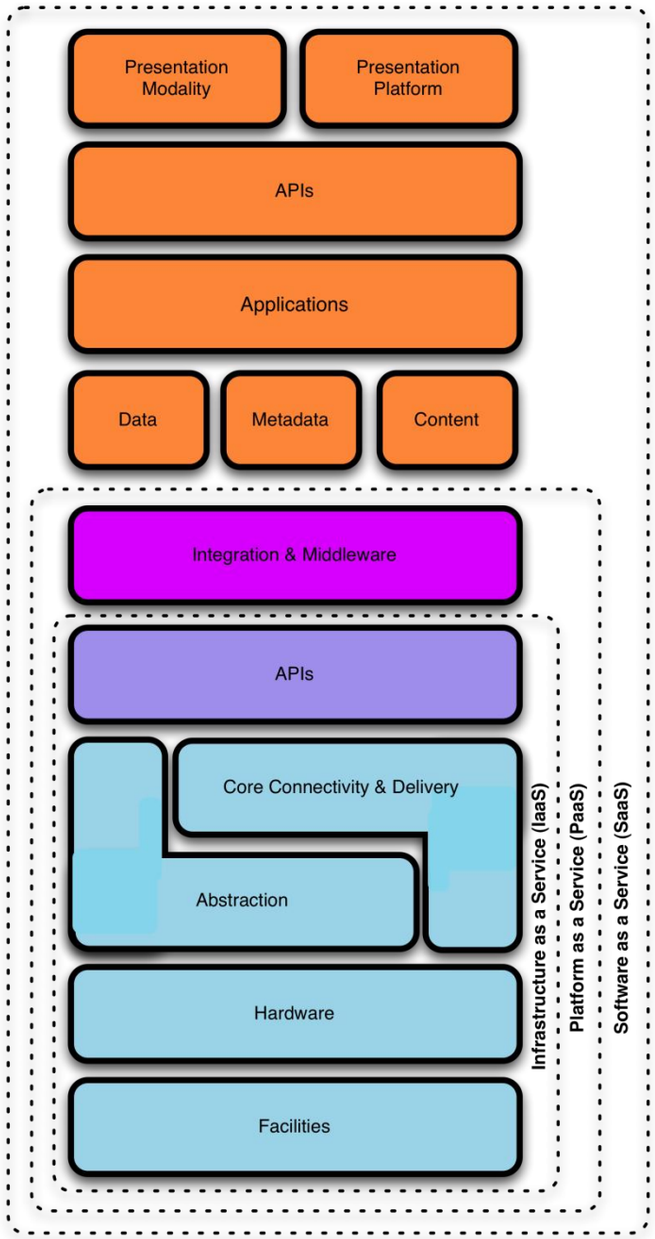


Essential Characteristics

Delivery Models

Deployment Models

What is Cloud Computing?



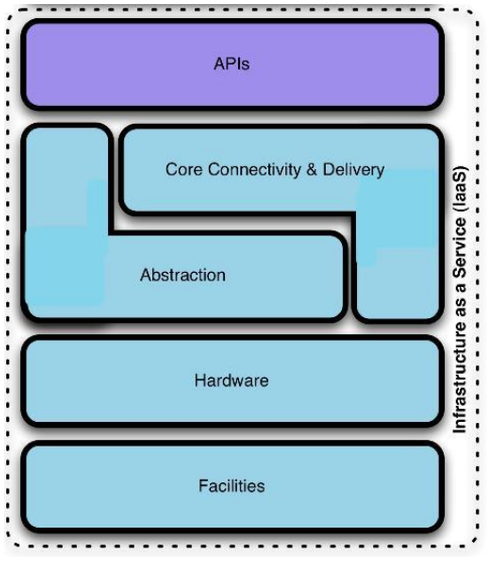
- CSA Cloud Reference Model
  - IaaS is the foundation
  - PaaS adds middleware to IaaS
  - SaaS represents complete applications on top of PaaS

S-P-I Model

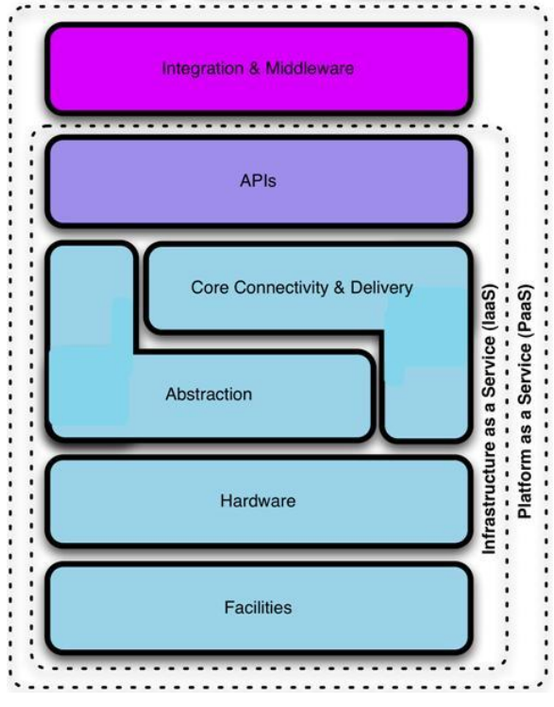
You build security in

You "RFP" security in

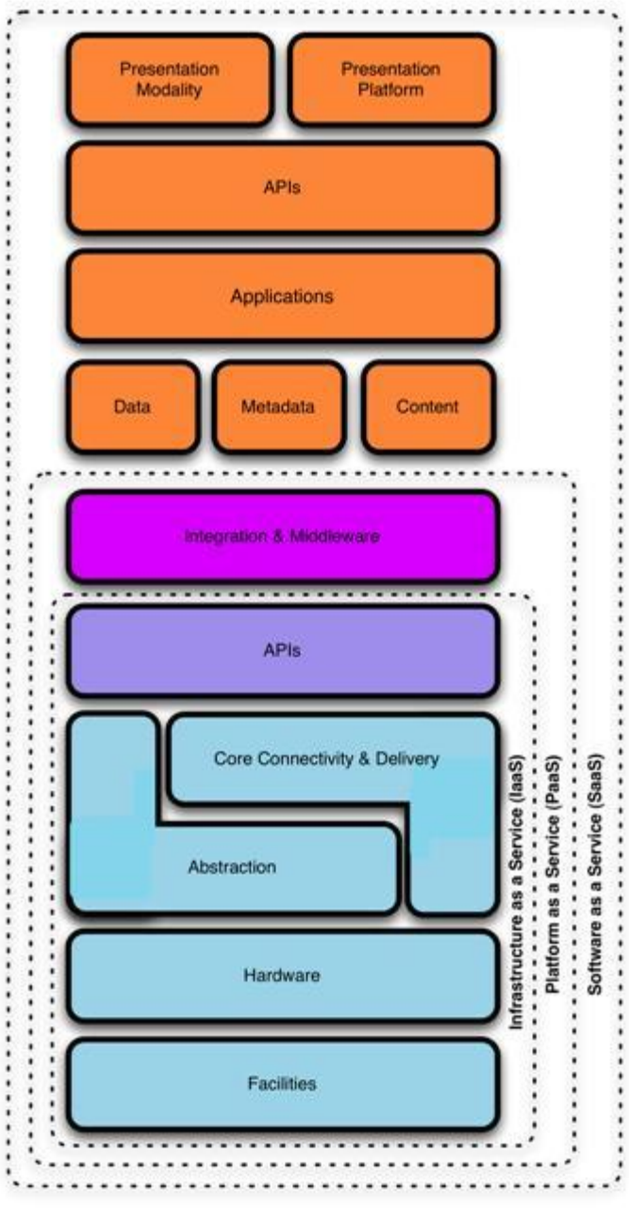
IaaS
Infrastructure as a Service



PaaS
Platform as a Service



SaaS
Software as a Service



cloud security alliance

www.cloudsecurityalliance.org

Cloud Computing Impacts

- Economic
  - Drives huge growth in computing
  - Spurs new business models
- Regulations
  - Compliance
  - Audit
- IT & IT Security professions
  - Skillset demands recalibrated between cloud providers and customers

Are there problems?

- Challenges abound – business can bypass IT
  - Perceptions of economic benefits rapidly gaining on perceptions of risk
- But… organizational verities remain:
  - Shareholder responsibility
  - Commitment to customers
  - Regulatory compliance
- We need to assure responsible and secure adoption of cloud

Governance!

Lots of Governance Issues

- Cloud Provider going out of business
- Provider not achieving SLAs
- Provider having poor business continuity planning
- Data Centers in countries with unfriendly laws
- Proprietary lock-in with technology, data formats
- Mistakes made by cloud provider's internal IT security – several orders of magnitude more serious

Can't I just call it Outsourcing?

- IaaS & PaaS – Definitely not!
  - Only parts of the solution, you supply the rest
- SaaS is closer to outsourcing, but…
  - Multi-Tenancy
  - Geo-anonymity, anonymity of provider
  - Duration of service highly irregular
- 100% logical controls, many of them brand new

Thinking about Threats

- Technology
  - Unvetted innovations within the S-P-I stack
  - Well known cloud architectures
- Business
  - How cloud dynamism is leveraged by customers/providers
  - E.g. provisioning, elasticity, load management
- Old threats reinvented: “must defend against the accumulation of all vulnerabilities ever recorded”, Dan Geer-ism
- Malware in the cloud, for the cloud
- Lots of blackbox testing

Evolving Threats

- Unprotected APIs / Insecure Service Oriented Architecture
- Hypervisor Attacks
- L1/L2 Attacks (Cache Scraping)
- Trojaned AMI Images
- VMDK / VHD Repurposing
- Key Scraping
- Infrastructure DDoS
- Web application (mgt interface!)
  - XSRF
  - XSS
  - SQL Injection
- Data leakage
- Poor account provisioning
- Cloud provider insider abuse
- Financial DDoS
- "Click Fraud”

About the Cloud Security Alliance

- Global, not-for-profit organization
- Inclusive membership, supporting broad spectrum of subject matter expertise: cloud experts, security, legal, compliance, virtualization, and on and on…
- We believe Cloud Computing has a robust future, we want to make it better

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

cloud security alliance

www.cloudsecurityalliance.org

What is the CSA strategy?

- Get ahead of the cloud security problem while adoption is modest
- Build awareness of the issues – deliver pragmatic guidance for today
- Partner with all key stakeholders who hold part of the solution
- Facilitate the adoption of standards
- Create an ecosystem that can make the cloud more secure than traditional IT

cloud security alliance

Some CSA Activities

- Partnering with ENISA to incorporate key EU concerns
- Collaboration with ISACA to drive IT audit education and tools
- Peer review of web-specific issues with OWASP
- Part of the Cloud Standards Coordination Wiki
  - Distributed Management Task Force (DMTF)
  - The European Telecommunications Standards Institute (ETSI)
  - National Institute of Standards and Technology (NIST)
  - Storage Networking Industry Association (SNIA)
  - Many more…

cloud security alliance

Some CSA Activities

- Creating worldwide chapters for global action
- Delivering version 2 of CSA Guidance in November 2009
- Working groups for industries, government & specific interests
- Cloud threats research and regular “top lists”
- Translating guidance
- Separate corporate memberships for cloud providers and cloud customers

Some results we are looking for

- Adaptation of security controls to new “100% logical” environment
- Mapping of frameworks to cloud (e.g. COBIT, ISO 27002, etc.)
- Certifications for cloud providers that mean something
- Updated understanding of concepts such as data, location
- Cloud-savvy IT Security professionals
- Build security into the cloud

CSA Guidance Domains

1. Understand Cloud Architecture

Governing in the Cloud

2. Governance & Risk Mgt
3. Legal
4. Electronic Discovery
5. Compliance & Audit
6. Information Lifecycle Mgt
7. Portability & Interoperability

Operating in the Cloud

8. Traditional, BCM, DR
9. Data Center Operations
10. Incident Response
11. Application Security
12. Encryption & Key Mgt
13. Identity & Access Mgt
14. Storage
15. Virtualisation

www.cloudsecurityalliance.org

Governance & ERM

- A portion of cloud cost savings must be invested into provider scrutiny
- Third party transparency of cloud provider
- Financial viability of cloud provider
- Understand provider's key risk & performance indicators and how to monitor

Legal & eDiscovery

- 3 Interdependent Dimensions: Functional, Jurisdictional, Contractual
- Plan for both an expected and unexpected termination of the relationship and an orderly return of your assets.
- Find conflicts between the laws the cloud provider must comply with and those governing the cloud customer
- Secondary uses of data
- Gain a clear expectation of the cloud provider's role & response to legal requests for information.
- Understand role of provider in eDiscovery scenarios
- Understand logging capabilities and Metadata

Compliance & Audit

- Classify data and systems to understand compliance requirements
- Cross border data transfers
- Maintain a right to audit on demand
- Need uniformity in comprehensive certification scoping to beef up SAS 70 II, ISO 2700X

Information Lifecycle Mgt

- Understand the logical segregation of information and protective controls implemented
- Data retention assurance easy, data destruction may be very difficult.
- Understand cloud provider storage retirement processes.
- Recovering true cost of a breach: penalties vs risk transference
- Can the cloud provider support long term archiving, will the data be available several years later?
- Do next generation cloud storage technologies bypass control domains?

Portability & Interoperability

- Understand and implement layers of abstraction
- For Platform as a Service (PaaS), careful architecture should be followed to minimize potential lock-in for the customer. “Loose coupling” using SOA principles
- Understand who the competitors are to your cloud providers and what their capabilities are to assist in migration
- Advocate open standards

Traditional, BCM/DR

- Greatest concern is insider threat
- Cloud providers should adopt as a security baseline the most stringent requirements of any customer
- Compartmentalization of job duties and limit knowledge of customers
- Inspect cloud provider disaster recovery and business continuity plans

Data Center Operations

- Know cloud provider's other clients to assess their impact on you
- Understand how resource sharing occurs within your cloud provider to understand impact during your business fluctuations.
- For IaaS and PaaS, the cloud provider's patch management policies and procedures have significant impact
- Cloud provider's technology architecture may use new and unproven methods for failover.

Incident Response

- Any data classified as private for the purpose of data breach regulations should always be encrypted to reduce the consequences of a breach incident.
- Logging: Cloud providers need application layer logging frameworks to provide granular narrowing of incidents to a specific customer.
- Cloud providers and customers need defined collaboration for incident response.

Application Security

- For IaaS, need trusted virtual machine images.
- Apply best practices available to harden DMZ host systems to virtual machines.
- Securing inter-host communications must be the rule, there can be no assumption of a secure channel between hosts
- Understand how malicious actors are likely to adapt their attack techniques to cloud platforms, e.g. increased black box testing

Encryption & Key Mgt

- From a risk management perspective, unencrypted data existent in the cloud may be considered “lost” by the customer.
- Use encryption to separate data holding from data usage.
- Segregate the key management from the cloud provider hosting the data, creating a chain of separation.
- Stipulate standard encryption in contract language

Identity & Access Mgt

- Must have a robust federated identity management architecture and strategy internal to the organization.
- Insist upon standards enabling federation: primarily SAML, WS-Federation and Liberty ID-FF federation
- Consider implementing Single Sign-on (SSO) for internal applications, and leveraging this architecture for cloud applications.
- Using cloud-based “Identity as a Service” providers may be a useful tool for abstracting and managing complexities such as differing versions of SAML, etc.

Virtualization

- Virtualized operating systems should be augmented by third party security technology.
- Secure by default configuration needs to be assured by following or exceeding available industry baselines.
- Need granular monitoring of traffic crossing VM backplanes
- Provisioning, administrative access and control of virtualized operating systems is crucial

Summary

- Cloud Computing is real and transformational
- Challenges for People, Process, Technology, Organizations and Countries
- Broad governance approach needed
- Tactical fixes needed
- Combination of updating existing best practices and creating completely new best practices
- Common sense not optional

cloud security alliance

Contact

- Help us secure cloud computing
- www.cloudsecurityalliance.org
- info@cloudsecurityalliance.org
- LinkedIn: www.linkedin.com/groups?gid=1864210
- Twitter: #cloudsa

Thank you!

cloud security alliance

www.cloudsecurityalliance.org