Assessing Risks in the Cloud

Jim Reavis

Executive Director

Cloud Security Alliance

CSA cloud security alliance℠

Agenda

- Definitions of Cloud & Cloud Usage
- Key Cloud Risks
- About CSA
- CSA Guidance approach to Addressing Risks
- Research Priorities

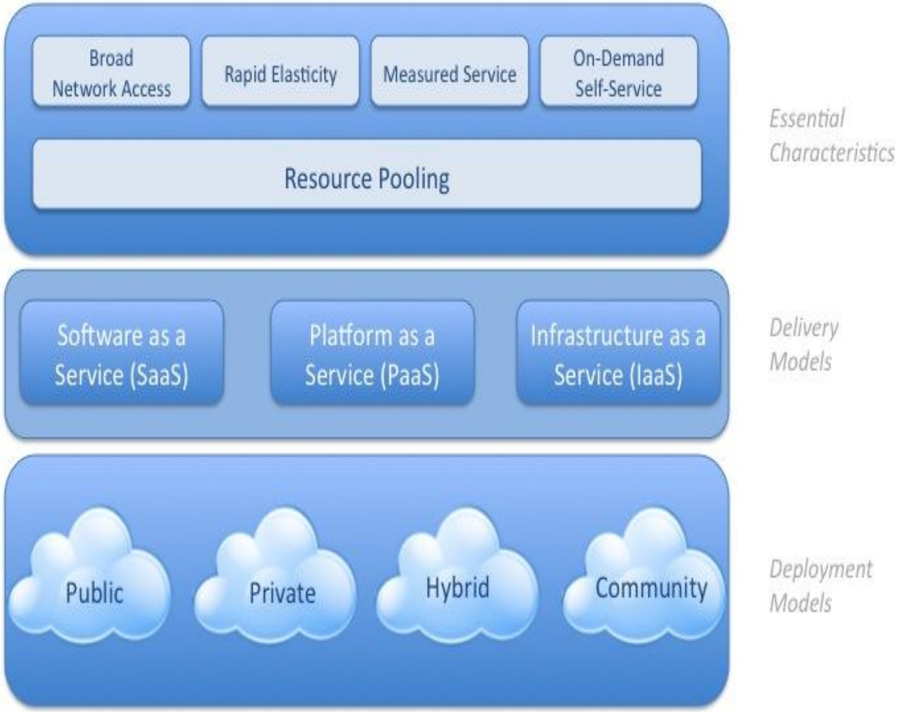
Cloud: Dawn of a New Age

- Art Coviello – “the most overhyped, underestimated phenomenon since the Internet”
- Compute as a utility
- Changes everything: Business models, venture capital, R&D, ……

What is Cloud Computing?

- Compute as a utility: Third major era of computing
- Cloud enabled by
  - Moore's Law
  - Hyperconnectivity
  - SOA
  - Provider scale
- Key characteristics
  - Elastic & on-demand
  - Multi-tenancy
  - Metered service
- Disrupts Everything!

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

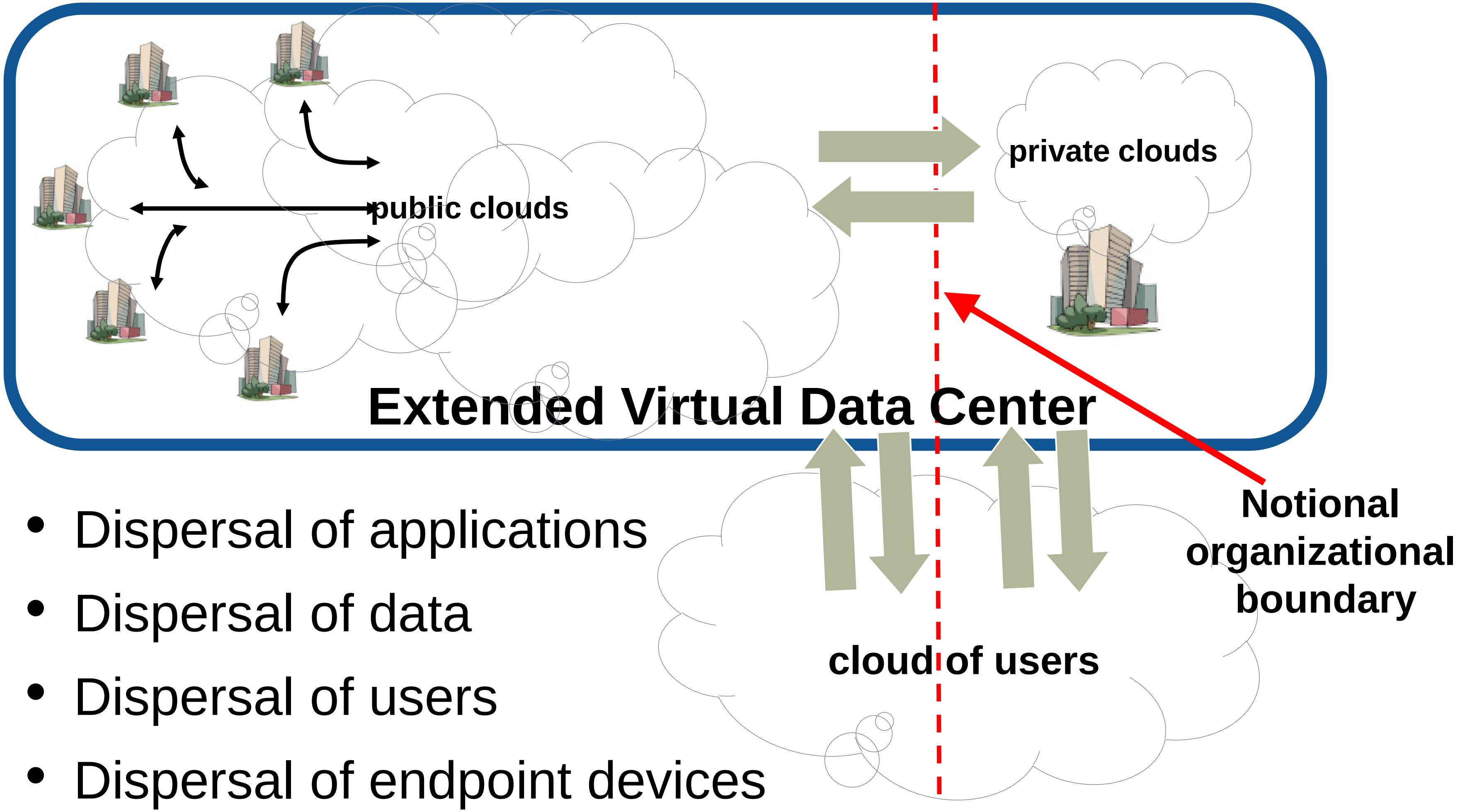


Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Delivery Models

Public
Private
Hybrid
Community
Deployment Models

2011-2014: the Hybrid Enterprise


public clouds
private clouds
Extended Virtual Data Center
cloud of users
Notional organizational boundary

- Dispersal of applications
- Dispersal of data
- Dispersal of users
- Dispersal of endpoint devices

Key Cloud Security Problems of Today

From CSA Top Threats Research:

- Trust: Lack of Provider transparency, impacts Governance, Risk Management, Compliance
- Data: Leakage, Loss or Storage in unfriendly geography
- Insecure Cloud software
- Malicious use of Cloud services
- Account/Service Hijacking
- Malicious Insiders
- Cloud-specific Attacks

Key Problems of Tomorrow

- Globally compatible legislation and policy
- Compatible private & public clouds
- Real-time risk management & compliance
- Identity management
- Responding to security incidents

Cloud: Reset Security Industry

- Critical mass of separation between data owners and data processors
- Cloud customers retain governance responsibility
- Physical controls must be replaced by virtual controls
- Opportunity to make security better
- Requires broad stakeholder perspective
- Must build the cloud security ecosystem

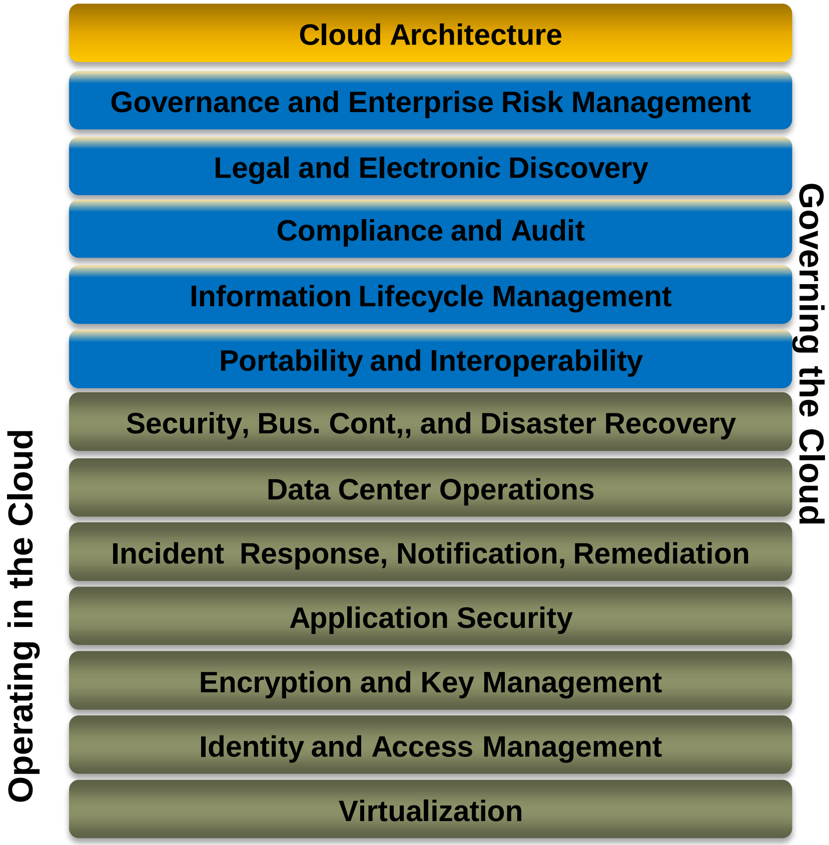
About the CSA

- Global, not-for-profit organization
- 15,000 individual members, 80 corporate members
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: Build using existing standards
  - Identity: A key foundation of a functioning cloud economy
  - Champion interoperability
  - Advocacy of prudent public policy

"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."

CSA Guidance Research

- Popular best practices for securing cloud computing
- 13 Domains of concern – governing & operating groupings
- Key to assessing and mitigating risks


Cloud Architecture
Governance and Enterprise Risk Management
Legal and Electronic Discovery
Compliance and Audit
Information Lifecycle Management
Portability and Interoperability
Security, Bus. Cont,, and Disaster Recovery
Data Center Operations
Incident Response, Notification, Remediation
Application Security
Encryption and Key Management
Identity and Access Management
Virtualization
Governing the Cloud
Operating in the Cloud

Guidance > 200k downloads: cloudsecurityalliance.org/guidance

Governance and ERM

- A portion of cloud cost savings must be invested into provider scrutiny
- Third party transparency of cloud provider
- Supply chain view of cloud provider’s services
- Financial viability of cloud provider
- Understand provider’s key risk & performance indicators and how to monitor
- More holistic view of provider’s business compared to software companies

Legal & eDiscovery

- 3 Interdependent Dimensions: Functional, Jurisdictional, Contractual
- Distinction from outsourcing: Transient service, anonymity of provider and geography
- 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 and response to legal requests for information
- 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
- Auditor qualifications
- Need uniformity in comprehensive certification scoping to beef up SAS 70 II, ISO 2700X
- Continuous monitoring

Information Lifecycle Management

- Data security lifecycle
  - Create → Store → Use
  - Share → Archive → Destroy
- Data remanence or persistence
- Commingling data with other customers
- Backup and recovery schemes
- Data discovery
- Data aggregation and inference

Portability and Interoperability

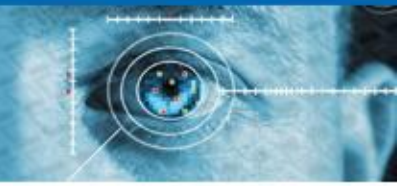
- Understand and implement layers of abstraction
- For PaaS, data should be portable. Careful architecture should be followed to minimize potential lock-in for the customer's application. "Loose coupling" using SOA principles
- For IaaS, data and applications should be portable
- For SaaS, focus is data portability and maintaining application feature requirements
- Advocate open standards
- Third-party cloud intermediaries and brokering

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. Standard and comprehensive logs
- Cloud providers and customers need defined collaboration for incident response.
- Snapshots of entire virtual environment
- Go back to known good state

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
- Updated threat models
- New trust domains for SDLC

Encryption and Key Management

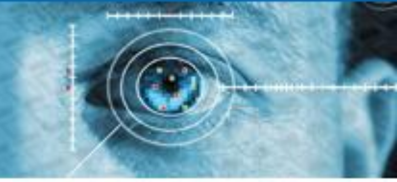
- From a risk management perspective, unencrypted data existent in the cloud may be considered “lost” by the customer.
- Use encryption to separate data holding from data usage.
- Segregate the key management from the cloud provider hosting the data, creating a chain of separation.
- Stipulate standard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

Identity and Access Management

- 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
- Cloud providers should by default be relying parties to trusted identity providers
- 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

- Understand VM attack vectors: Hypervisor, backplane, hardware, provisioning, other management tools
- 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



CSA Research

- CSA Guidance Version 3 (Security as a Service)
- GRC Stack
  - CloudAudit
  - Cloud Controls Matrix
  - Consensus Assessments Initiative
- CloudCERT
- Trusted Cloud Initiative
- CCSK – Certificate of Cloud Security Knowledge
- Industry-specific working groups

Public Policy

- Harmonize global privacy directives
- “Safe Harbor” exemptions updated for cloud
- National strategies aligned with international strategies
- “G20-type” Summit to pursue global cloud policy issues
- Pursuit of criminal organizations

Thank you

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

CSA cloud security alliance SM